BULLETIN (SB24-309)

VULNERABILITY SUMMARY FOR THE WEEK OF

28TH OCTOBER, 2024

Bulletin (SB24-309)
Vulnerability Summary for the Week of October 28, 2024

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High- Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.
Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0.6.9 -
Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Admin--Verbalize WP	Unrestricted Upload of File with Dangerous Type vulnerability in Admin Verbalize WP Upload a Web Shell to a Web Server.This issue affects Verbalize WP: from n/a through 1.0.	2024-10-23	10	CVE-2024-49668
advancedcoding--Comments wpDiscuz	The Comments - wpDiscuz plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 7.6.24. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not have an already-existing account for the service returning the token.	2024-10-25	9.8	CVE-2024-9488
Alexander De Ridder--INK Official	Unrestricted Upload of File with Dangerous Type vulnerability in Alexander De Ridder INK Official allows Upload a Web Shell to a Web Server.This issue affects INK Official: from n/a through 4.1.2.	2024-10-23	9.9	CVE-2024-49669
Amazon--Amazon.ApplicationLoadBalancer.Identity.AspNetCore Middleware	The Amazon.ApplicationLoadBalancer.Identity.AspNetCore repo https://github.com/awslabs/aws-alb-identity-aspnetcore#validatetokensignature contains Middleware that can be used in conjunction with the Application Load Balancer (ALB) OpenId Connect integration and can be used in any ASP.NET https://dotnet.microsoft.com/apps/aspnet Core deployment scenario, including Fargate, EKS, ECS, EC2, and Lambda. In the JWT handling code, it performs signature validation but fails to validate the JWT issuer and signer identity. The signer omission, if combined with a scenario where the infrastructure owner allows internet traffic to the ALB targets (not a recommended configuration), can allow for JWT signing by an untrusted entity and an actor may be able to mimic valid OIDC-federated sessions to the ALB targets. The repository/package has been deprecated, is end of life, and is no longer supported. As a security best practice, ensure that your ELB targets (e.g. EC2 Instances, Fargate Tasks etc.) do not have public IP addresses. Ensure any forked or derivative code validate that the signer attribute in the JWT match the ARN of the Application Load Balancer that the service is configured to use.	2024-10-22	7.5	CVE-2024-10125
Amazon--AWS ALB Route Directive Adapter For Istio	The AWS ALB Route Directive Adapter For Istio repo https://github.com/awslabs/aws-alb-route-directive-adapter-for-istio/tree/master provides an OIDC authentication mechanism that was integrated into the open source Kubeflow project. The adapter uses JWT for authentication, but lacks proper signer and issuer validation. In deployments of ALB that ignore security best practices, where ALB targets are directly exposed to internet traffic, an actor can provide a JWT signed by an untrusted entity in order to spoof OIDC-federated sessions and successfully bypass authentication. The repository/package has been deprecated, is end of life, and is no longer supported. As a security best practice, ensure that your ELB targets (e.g. EC2 Instances, Fargate Tasks etc.) do not have public IP addresses. Ensure any forked or derivative code validate that the signer attribute in the JWT match the ARN of the Application Load Balancer that the service is configured to use.	2024-10-22	7.5	CVE-2024-8901
appcheap--App Builder Create Native Android & iOS Apps On The Flight	The App Builder - Create Native Android & iOS Apps On The Flight plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 5.3.7. This is due to the verify_otp_forgot_password() and update_password() functions not having enough controls to prevent a successful brute force attack of the OTP to change a password, or verify that a password reset request came from an authorized user. This makes it possible for unauthenticated attackers to generate and brute force an OTP that makes it possible to change any users passwords, including an administrator.	2024-10-25	8.1	CVE-2024-9302
baserproject--basercms	baserCMS is a website development framework. Versions prior to 5.1.2 have a cross-site scripting vulnerability in the Edit Email Form Settings Feature. Version 5.1.2 fixes the issue.	2024-10-24	7.1	CVE-2024-46998

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
buddypress--BuddyPress	The BuddyPress plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 14.1.0 via the id parameter. This makes it possible for authenticated attackers, with Subscriber-level access and above, to perform actions on files outside of the originally intended directory and enables file uploads to directories outside of the web root. Depending on server configuration it may be possible to upload files with double extensions. This vulnerability only affects Windows.	2024-10-25	8.1	CVE-2024-10011
Cisco--Cisco Adaptive Security Appliance (ASA) Software	A vulnerability in the SSH subsystem of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to execute operating system commands as root. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by submitting crafted input when executing remote CLI commands over SSH. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system.	2024-10-23	9.9	CVE-2024-20329
Cisco--Cisco Adaptive Security Appliance (ASA) Software	A vulnerability in the VPN and management web servers of the Cisco Adaptive Security Virtual Appliance (ASAv) and Cisco Secure Firewall Threat Defense Virtual (FTDv), formerly Cisco Firepower Threat Defense Virtual, platforms could allow an unauthenticated, remote attacker to cause the virtual devices to run out of system memory, which could cause SSL VPN connection processing to slow down and eventually cease all together. This vulnerability is due to a lack of proper memory management for new incoming SSL/TLS connections on the virtual platforms. An attacker could exploit this vulnerability by sending a large number of new incoming SSL/TLS connections to the targeted virtual platform. A successful exploit could allow the attacker to deplete system memory, resulting in a denial of service (DoS) condition. The memory could be reclaimed slowly if the attack traffic is stopped, but a manual reload may be required to restore operations quickly.	2024-10-23	8.6	CVE-2024-20260
Cisco--Cisco Adaptive Security Appliance (ASA) Software	A vulnerability in the SSL VPN feature for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to a logic error in memory management when the device is handling SSL VPN connections. An attacker could exploit this vulnerability by sending crafted SSL/TLS packets to the SSL VPN server of the affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	2024-10-23	8.6	CVE-2024-20402
Cisco--Cisco Adaptive Security Appliance (ASA) Software	A vulnerability in the Internet Key Exchange version 2 (IKEv2) protocol for VPN termination of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted IKEv2 traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	2024-10-23	8.6	CVE-2024-20426
Cisco--Cisco Adaptive Security Appliance (ASA) Software	A vulnerability in the TLS cryptography functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper data validation during the TLS 1.3 handshake. An attacker could exploit this vulnerability by sending a crafted TLS 1.3 packet to an affected system through a TLS 1.3-enabled listening socket. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: This vulnerability can also impact the integrity of a device by causing VPN HostScan	2024-10-23	8.6	CVE-2024-20494

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	communication failures or file transfer failures when Cisco ASA Software is upgraded using Cisco Adaptive Security Device Manager (ASDM).			
Cisco--Cisco Adaptive Security Appliance (ASA) Software	A vulnerability in the Remote Access VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition on an affected device. This vulnerability is due to improper validation of client key data after the TLS session is established. An attacker could exploit this vulnerability by sending a crafted key value to an affected system over the secure TLS session. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	2024-10-23	8.6	CVE-2024-20495
Cisco--Cisco Adaptive Security Appliance (ASA) Software	A vulnerability in the Simple Network Management Protocol (SNMP) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause an unexpected reload of the device. This vulnerability is due to insufficient input validation of SNMP packets. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device using IPv4 or IPv6. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability affects all versions of SNMP (versions 1, 2c, and 3) and requires a valid SNMP community string or valid SNMPv3 user credentials.	2024-10-23	7.7	CVE-2024-20268
Cisco--Cisco Adaptive Security Appliance (ASA) Software	A vulnerability in the Dynamic Access Policies (DAP) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause an affected device to reload unexpectedly. To exploit this vulnerability, an attacker would need valid remote access VPN user credentials on the affected device. This vulnerability is due to improper validation of data in HTTPS POST requests. An attacker could exploit this vulnerability by sending a crafted HTTPS POST request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition.	2024-10-23	7.7	CVE-2024-20408
Cisco--Cisco Firepower Management Center	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Software, could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system as root. This vulnerability is due to insufficient input validation of certain HTTP requests. An attacker could exploit this vulnerability by authenticating to the web-based management interface of an affected device and then sending a crafted HTTP request to the device. A successful exploit could allow the attacker to execute arbitrary commands with root permissions on the underlying operating system of the Cisco FMC device or to execute commands on managed Cisco Firepower Threat Defense (FTD) devices. To exploit this vulnerability, the attacker would need valid credentials for a user account with at least the role of Security Analyst (Read Only).	2024-10-23	9.9	CVE-2024-20424
Cisco--Cisco Firepower Threat Defense Software	A vulnerability in Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000, 2100, 3100, and 4200 Series could allow an unauthenticated, local attacker to access an affected system using static credentials. This vulnerability is due to the presence of static accounts with hard-coded passwords on an affected system. An attacker could exploit this vulnerability by logging in to the CLI of an affected device with these credentials. A successful exploit could allow the attacker to access the affected system and retrieve sensitive information, perform limited troubleshooting actions, modify some configuration options, or render the device unable to boot to the operating system, requiring a reimage of the device.	2024-10-23	9.3	CVE-2024-20412
Cisco--Cisco Firepower Threat	A vulnerability in the Snort 2 and Snort 3 TCP and UDP detection engine of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series Appliances could allow an unauthenticated, remote attacker to cause memory	2024-10-23	8.6	CVE-2024-20330

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Defense Software	corruption, which could cause the Snort detection engine to restart unexpectedly. This vulnerability is due to improper memory management when the Snort detection engine processes specific TCP or UDP packets. An attacker could exploit this vulnerability by sending crafted TCP or UDP packets through a device that is inspecting traffic using the Snort detection engine. A successful exploit could allow the attacker to restart the Snort detection engine repeatedly, which could cause a denial of service (DoS) condition. The DoS condition impacts only the traffic through the device that is examined by the Snort detection engine. The device can still be managed over the network. Note: Once a memory block is corrupted, it cannot be cleared until the Cisco Firepower 2100 Series Appliance is manually reloaded. This means that the Snort detection engine could crash repeatedly, causing traffic that is processed by the Snort detection engine to be dropped until the device is manually reloaded.			
Cisco--Cisco Firepower Threat Defense Software	A vulnerability in the TLS processing feature of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to an issue that occurs when TLS traffic is processed. An attacker could exploit this vulnerability by sending certain TLS traffic over IPv4 through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition and impacting traffic to and through the affected device.	2024-10-23	8.6	CVE-2024-20339
Cisco--Cisco Firepower Threat Defense Software	A vulnerability in the TCP/IP traffic handling function of the Snort Detection Engine of Cisco Firepower Threat Defense (FTD) Software and Cisco FirePOWER Services could allow an unauthenticated, remote attacker to cause legitimate network traffic to be dropped, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of TCP/IP network traffic. An attacker could exploit this vulnerability by sending a large amount of TCP/IP network traffic through the affected device. A successful exploit could allow the attacker to cause the Cisco FTD device to drop network traffic, resulting in a DoS condition. The affected device must be rebooted to resolve the DoS condition.	2024-10-23	8.6	CVE-2024-20351
code-projects -- pharmacy_management_system	A vulnerability was found in code-projects Pharmacy Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /add_new_invoice.php. The manipulation of the argument text leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-21	9.8	CVE-2024-10196
Codezips--Pet Shop Management System	A vulnerability, which was classified as critical, has been found in Codezips Pet Shop Management System 1.0. This issue affects some unknown processing of the file /animalsupdate.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-27	7.3	CVE-2024-10430
Codezips--Pet Shop Management System	A vulnerability, which was classified as critical, was found in Codezips Pet Shop Management System 1.0. Affected is an unknown function of the file /deletebird.php. The manipulation of the argument t1 leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-27	7.3	CVE-2024-10431
Codezips--Sales Management System	A vulnerability was found in Codezips Sales Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /addstock.php. The manipulation of the argument prodtype leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-25	7.3	CVE-2024-10368
Codezips--Sales Management System	A vulnerability was found in Codezips Sales Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /addcustcom.php. The manipulation of the argument refno leads to sql	2024-10-25	7.3	CVE-2024-10369

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.			
Codezips--Sales Management System	A vulnerability was found in Codezips Sales Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /addcustind.php. The manipulation of the argument refno leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-25	7.3	CVE-2024-10370
delabon--WordPress Post Grid Layouts with Pagination Sogrid	The WordPress Post Grid Layouts with Pagination - Sogrid plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.5.2 via the 'tab' parameter. This makes it possible for authenticated attackers, with Administrator-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included. This can also be exploited via CSRF techniques.	2024-10-26	7.2	CVE-2024-8392
deryck--User Toolkit	The User Toolkit plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.2.3. This is due to an improper capability check in the 'switchUser' function. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to log in as any existing user on the site, such as an administrator.	2024-10-26	8.8	CVE-2024-9890
Dogu Pekgoz--AI Image Generator for Your Content & Featured Images AI Postpix	Unrestricted Upload of File with Dangerous Type vulnerability in Dogu Pekgoz AI Image Generator for Your Content & Featured Images - AI Postpix allows Upload a Web Shell to a Web Server.This issue affects AI Image Generator for Your Content & Featured Images - AI Postpix: from n/a through 1.1.8.	2024-10-23	9.9	CVE-2024-49671
Ecomerciar--Woocommerce Custom Profile Picture	Unrestricted Upload of File with Dangerous Type vulnerability in Ecomerciar Woocommerce Custom Profile Picture allows Upload a Web Shell to a Web Server.This issue affects Woocommerce Custom Profile Picture: from n/a through 1.0.	2024-10-23	9.9	CVE-2024-49658
elecom -- wab-i1750-ps_firmware	Stack-based buffer overflow vulnerability exists in WAB-I1750-PS and WAB-S1167-PS. By processing a specially crafted HTTP request, arbitrary code may be executed.	2024-10-21	9.8	CVE-2024-43689
fortinet -- fortimanager	A missing authentication for critical function in FortiManager 7.6.0, FortiManager 7.4.0 through 7.4.4, FortiManager 7.2.0 through 7.2.7, FortiManager 7.0.0 through 7.0.12, FortiManager 6.4.0 through 6.4.14, FortiManager 6.2.0 through 6.2.12, Fortinet FortiManager Cloud 7.4.1 through 7.4.4, FortiManager Cloud 7.2.1 through 7.2.7, FortiManager Cloud 7.0.1 through 7.0.13, FortiManager Cloud 6.4.1 through 6.4.7 allows attacker to execute arbitrary code or commands via specially crafted requests.	2024-10-23	9.8	CVE-2024-47575
funnelkit -- funnelkit_automations	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in FunnelKit Automation By Autonami allows SQL Injection.This issue affects Automation By Autonami: from n/a through 3.1.2.	2024-10-21	7.2	CVE-2024-47328
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 15.10 before 17.3.6, 17.4 before 17.4.3, and 17.5 before 17.5.1. An attacker could inject HTML into the Global Search field on a diff view leading to XSS.	2024-10-24	8.7	CVE-2024-8312

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	there is a possible man-in-the-middle attack due to a logic error in the code. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	8.1	CVE-2024-47023
google -- android	Android before 2024-10-05 on Google Pixel devices allows information disclosure in the modem component, A-299774545.	2024-10-25	7.5	CVE-2024-44100
google -- android	there is a possible Null Pointer Dereference (modem crash) due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.5	CVE-2024-44101
google -- android	In mm_GetMobileIdIndexForNsUpdate of mm_GmmPduCodec.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.8	CVE-2024-47012
google -- android	Android before 2024-10-05 on Google Pixel devices allows information disclosure in the ABL component, A-331966488.	2024-10-25	7.5	CVE-2024-47020
google -- android	In sms_ExtractCbLanguage of sms_CellBroadcast.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.5	CVE-2024-47021
google -- android	Android before 2024-10-05 on Google Pixel devices allows information disclosure in the ACPM component, A-331255656.	2024-10-25	7.5	CVE-2024-47022
google -- chrome	Inappropriate implementation in Extensions in Google Chrome prior to 130.0.6723.69 allowed a remote attacker to bypass site isolation via a crafted Chrome Extension. (Chromium security severity: High)	2024-10-22	8.1	CVE-2024-10229
google -- chrome	Type Confusion in V8 in Google Chrome prior to 130.0.6723.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-10-22	8.8	CVE-2024-10230
google -- chrome	Type Confusion in V8 in Google Chrome prior to 130.0.6723.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-10-22	8.8	CVE-2024-10231
Google--Android	Android before 2024-10-05 on Google Pixel devices allows privilege escalation in the ABL component, A-330537292.	2024-10-25	8.8	CVE-2024-47014
Google--Android	In lwis_device_event_states_clear_locked of lwis_event.c, there is a possible privilege escalation due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.4	CVE-2024-44098
Google--Android	In pmucal_rae_handle_seq_int of flexpmu_cal_rae.c, there is a possible arbitrary write due to uninitialized data. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.8	CVE-2024-47013
Google--Android	there is a possible privilege escalation due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.8	CVE-2024-47016
Google--Android	In ufshc_scsi_cmd of ufs.c, there is a possible stack variable use after free due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.8	CVE-2024-47017

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Google--Android	In vring_size of external/headers/include/virtio/virtio_ring.h, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.4	CVE-2024-47024
Google--Android	In sm_mem_compat_get_vmm_obj of lib/sm/shared_mem.c, there is a possible arbitrary physical memory access due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.4	CVE-2024-47027
Google--Android	In lwis_allocator_free of lwis_allocator.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.4	CVE-2024-47033
Google--Android	In vring_init of external/headers/include/virtio/virtio_ring.h, there is a possible out of bounds write due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.4	CVE-2024-47035
Google--Android	In valid_address of syscall.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-10-25	7.4	CVE-2024-47041
ibm -- concert	IBM Concert 1.0.0 and 1.0.1 vulnerable to attacks that rely on the use of cookies without the SameSite attribute.	2024-10-22	9.8	CVE-2024-43177
IceWhaleTech--ZimaOS	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.2.4 and all prior versions, the ZimaOS API endpoint `http://<Zima_Server_IP:PORT>/v3/file?token=<token>&files=<file_path>` is vulnerable to arbitrary file reading due to improper input validation. By manipulating the `files` parameter, authenticated users can read sensitive system files, including `/etc/shadow`, which contains password hashes for all users. This vulnerability exposes critical system data and poses a high risk for privilege escalation or system compromise. The vulnerability occurs because the API endpoint does not validate or restrict file paths provided via the `files` parameter. An attacker can exploit this by manipulating the file path to access sensitive files outside the intended directory. As of time of publication, no known patched versions are available.	2024-10-24	7.5	CVE-2024-48931
IceWhaleTech--ZimaOS	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.2.4 and all prior versions, the API endpoints in ZimaOS, such as `http://<Server-IP>/v1/users/image?path=/var/lib/casaos/1/app_order.json` and `http://<Server-IP>/v1/users/image?path=/var/lib/casaos/1/system.json`, expose sensitive data like installed applications and system information without requiring any authentication or authorization. This sensitive data leak can be exploited by attackers to gain detailed knowledge about the system setup, installed applications, and other critical information. As of time of publication, no known patched versions are available.	2024-10-24	7.5	CVE-2024-49357
IceWhaleTech--ZimaOS	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.2.4 and all prior versions, the API endpoint `http://<Zima_Server_IP:PORT>/v2_1/file` in ZimaOS is vulnerable to a directory traversal attack, allowing authenticated users to list the contents of any directory on the server. By manipulating the path parameter, attackers can access sensitive system directories such as `/etc`, potentially exposing critical configuration files and increasing the risk of further attacks. As of time of publication, no known patched versions are available.	2024-10-24	7.5	CVE-2024-49359

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
iniNet Solutions--SpiderControl SCADA PC HMI Editor	iniNet Solutions SpiderControl SCADA PC HMI Editor has a path traversal vulnerability. When the software loads a malicious 'ems' project template file constructed by an attacker, it can write files to arbitrary directories. This can lead to overwriting system files, causing system paralysis, or writing to startup items, resulting in remote control.	2024-10-24	8	CVE-2024-10313
James Eggers--Portfolleo	Unrestricted Upload of File with Dangerous Type vulnerability in James Eggers Portfolleo portfolleo allows Upload a Web Shell to a Web Server.This issue affects Portfolleo: from n/a through 1.2.	2024-10-23	9.9	CVE-2024-49653
janobe --online_complaint_site	SQL Injection vulnerability in Online Complaint Site v.1.0 allows a remote attacker to escalate privileges via the username and password parameters in the /admin.index.php component.	2024-10-22	9.8	CVE-2024-44812
jdsofttech--School Management System WPSchoolPress	The School Management System - WPSchoolPress plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.2.10. This is due to the plugin not properly validating a user's identity prior to updating their details like email. This makes it possible for authenticated attackers, with teacher-level access and above, to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account.	2024-10-26	8.8	CVE-2024-9637
jurredeklijn--Wux Blog Editor	The Wux Blog Editor plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.0.0. This is due to missing validation on the token being supplied during the autologin through the plugin. This makes it possible for unauthenticated attackers to log in to the first administrator user.	2024-10-26	9.8	CVE-2024-9931
jurredeklijn--Wux Blog Editor	The Wux Blog Editor plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'wuxbt_insertImageNew' function in versions up to, and including, 3.0.0. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-10-26	9.8	CVE-2024-9932
keith-cullen --freecoap	Null Pointer Dereference in `coap_client_exchange_blockwise2` function in Keith Cullen FreeCoAP 1.0 allows remote attackers to cause a denial of service and potentially execute arbitrary code via a specially crafted CoAP packet that causes `coap_msg_get_payload(resp)` to return a null pointer, which is then dereferenced in a call to `memcpy`.	2024-10-22	9.8	CVE-2024-40493
Kieback & Peter--DDC4040e	Kieback & Peter's DDC4000 series is vulnerable to a path traversal vulnerability, which may allow an unauthenticated attacker to read files on the system.	2024-10-22	9.8	CVE-2024-41717
Kieback&Peter--DDC4040e	Kieback & Peter's DDC4000 series uses weak credentials, which may allow an unauthenticated attacker to get full admin rights on the system.	2024-10-22	9.8	CVE-2024-43698
Kieback&Peter--DDC4040e	Kieback & Peter's DDC4000 series has an insufficiently protected credentials vulnerability, which may allow an unauthenticated attacker with access to /etc/passwd to read the password hashes of all users on the system.	2024-10-22	8.4	CVE-2024-43812
latepoint --latepoint	Cross-Site Request Forgery (CSRF) vulnerability in Latepoint LatePoint allows Cross Site Request Forgery.This issue affects LatePoint: from n/a through 4.9.91.	2024-10-21	8.8	CVE-2024-43945
Lawo AG--vsm LTC Time Sync (vTimeSync)	The web server of Lawo AG vsm LTC Time Sync (vTimeSync) is affected by a "..." (triple dot) path traversal vulnerability. By sending a specially crafted HTTP request, an unauthenticated remote attacker could download arbitrary files from the operating system. As a limitation, the exploitation is only possible if the requested file has some file extension, e. g. .exe or .txt.	2024-10-24	7.5	CVE-2024-6049

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Liferay--Portal	The workflow component in Liferay Portal 7.3.2 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, 7.4 GA through update 92 and 7.3 GA through update 36 does not properly check user permissions before updating a workflow definition, which allows remote authenticated users to modify workflow definitions and execute arbitrary code (RCE) via the headless API.	2024-10-22	9	CVE-2024-38002
Liferay--Portal	The Script Console in Liferay Portal 7.0.0 through 7.4.3.101, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, 7.2 GA through fix pack 20, 7.1 GA through fix pack 28, 7.0 GA through fix pack 102 and 6.2 GA through fix pack 173 does not sufficiently protect against Cross-Site Request Forgery (CSRF) attacks, which allows remote attackers to execute arbitrary Groovy script via a crafted URL or a XSS vulnerability.	2024-10-22	9.6	CVE-2024-8980
Liferay--Portal	Cross-site request forgery (CSRF) vulnerability in the My Account widget in Liferay Portal 7.4.3.75 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.2, 2023.Q3.1 through 2023.Q3.5, 7.4 update 75 through update 92 and 7.3 update 32 through update 36 allows remote attackers to (1) change user passwords, (2) shut down the server, (3) execute arbitrary code in the scripting console, (4) and perform other administrative actions via the _com_liferay_my_account_web_portlet_MyAccountPortlet_backURL parameter.	2024-10-22	8.8	CVE-2024-26271
Liferay--Portal	Cross-site request forgery (CSRF) vulnerability in the content page editor in Liferay Portal 7.3.2 through 7.4.3.107, and Liferay DXP 2023.Q4.0 through 2023.Q4.2, 2023.Q3.1 through 2023.Q3.5, 7.4 GA through update 92 and 7.3 GA through update 35 allows remote attackers to (1) change user passwords, (2) shut down the server, (3) execute arbitrary code in the scripting console, (4) and perform other administrative actions via the p_l_back_url parameter.	2024-10-22	8.8	CVE-2024-26272
Liferay--Portal	Cross-site request forgery (CSRF) vulnerability in the content page editor in Liferay Portal 7.4.0 through 7.4.3.103, and Liferay DXP 2023.Q4.0 through 2023.Q4.2, 2023.Q3.1 through 2023.Q3.5, 7.4 GA through update 92 and 7.3 update 29 through update 35 allows remote attackers to (1) change user passwords, (2) shut down the server, (3) execute arbitrary code in the scripting console, (4) and perform other administrative actions via the _com_liferay_commerce_catalog_web_internal_portlet_CommerceCatalogsPortlet_redirect parameter.	2024-10-22	8.8	CVE-2024-26273
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_reject_ipv6: fix nf_reject_ip6_tcphdr_put() syzbot reported that nf_reject_ip6_tcphdr_put() was possibly sending garbage on the four reserved tcp bits (th->res1) Use skb_put_zero() to clear the whole TCP header, as done in nf_reject_ip_tcphdr_put() BUG: KMSAN: uninit-value in nf_reject_ip6_tcphdr_put+0x688/0x6c0 net/ipv6/netfilter/nf_reject_ipv6.c:255 nf_reject_ip6_tcphdr_put+0x688/0x6c0 net/ipv6/netfilter/nf_reject_ipv6.c:255 nf_send_reset6+0xd84/0x15b0 net/ipv6/netfilter/nf_reject_ipv6.c:344 nft_reject_inet_eval+0x3c1/0x880 net/netfilter/nft_reject_inet.c:48 expr_call_ops_eval net/netfilter/nf_tables_core.c:240 [inline] nft_do_chain+0x438/0x22a0 net/netfilter/nf_tables_core.c:288 nft_do_chain_inet+0x41a/0x4f0 net/netfilter/nft_chain_filter.c:161 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xf4/0x400 net/netfilter/core.c:626 nf_hook include/linux/netfilter.h:269 [inline] NF_HOOK include/linux/netfilter.h:312 [inline] ipv6_rcv+0x29b/0x390 net/ipv6/ip6_input.c:310 __netif_receive_skb_one_core net/core/dev.c:5661 [inline] __netif_receive_skb+0x1da/0xa00 net/core/dev.c:5775 process_backlog+0x4ad/0xa50 net/core/dev.c:6108 __napi_poll+0xe7/0x980 net/core/dev.c:6772 napi_poll net/core/dev.c:6841 [inline] net_rx_action+0xa5a/0x19b0 net/core/dev.c:6963 handle_softirqs+0x1ce/0x800 kernel/softirq.c:554 __do_softirq+0x14/0x1a kernel/softirq.c:588 do_softirq+0x9a/0x100 kernel/softirq.c:455 __local_bh_enable_ip+0x9f/0xb0	2024-10-21	9.1	CVE-2024-47685

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	kernel/softirq.c:382 local_bh_enable include/linux/bottom_half.h:33 [inline] rcu_read_unlock_bh include/linux/rcupdate.h:908 [inline] __dev_queue_xmit+0x2692/0x5610 net/core/dev.c:4450 dev_queue_xmit include/linux/netdevice.h:3105 [inline] neigh_resolve_output+0x9ca/0xae0 net/core/neighbour.c:1565 neigh_output include/net/neighbour.h:542 [inline] ip6_finish_output2+0x2347/0x2ba0 net/ipv6/ip6_output.c:141 __ip6_finish_output net/ipv6/ip6_output.c:215 [inline] ip6_finish_output+0xbb8/0x14b0 net/ipv6/ip6_output.c:226 NF_HOOK_COND include/linux/netfilter.h:303 [inline] ip6_output+0x356/0x620 net/ipv6/ip6_output.c:247 dst_output include/net/dst.h:450 [inline] NF_HOOK include/linux/netfilter.h:314 [inline] ip6_xmit+0x1ba6/0x25d0 net/ipv6/ip6_output.c:366 inet6_csk_xmit+0x442/0x530 net/ipv6/inet6_connection_sock.c:135 __tcp_transmit_skb+0x3b07/0x4880 net/ipv4/tcp_output.c:1466 tcp_transmit_skb net/ipv4/tcp_output.c:1484 [inline] tcp_connect+0x35b6/0x7130 net/ipv4/tcp_output.c:4143 tcp_v6_connect+0x1bcc/0x1e40 net/ipv6/tcp_ipv6.c:333 __inet_stream_connect+0x2ef/0x1730 net/ipv4/af_inet.c:679 inet_stream_connect+0x6a/0xd0 net/ipv4/af_inet.c:750 __sys_connect_file net/socket.c:2061 [inline] __sys_connect+0x606/0x690 net/socket.c:2078 __do_sys_connect net/socket.c:2088 [inline] __se_sys_connect net/socket.c:2085 [inline] __x64_sys_connect+0x91/0xe0 net/socket.c:2085 x64_sys_call+0x27a5/0x3ba0 arch/x86/include/generated/asm/syscalls_64.h:43 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was stored to memory at: nf_reject_ip6_tcphdr_put+0x60c/0x6c0 net/ipv6/netfilter/nf_reject_ipv6.c:249 nf_send_reset6+0xd84/0x15b0 net/ipv6/netfilter/nf_reject_ipv6.c:344 nft_reject_inet_eval+0x3c1/0x880 net/netfilter/nft_reject_inet.c:48 expr_call_ops_eval net/netfilter/nf_tables_core.c:240 [inline] nft_do_chain+0x438/0x22a0 net/netfilter/nf_tables_core.c:288 nft_do_chain_inet+0x41a/0x4f0 net/netfilter/nft_chain_filter.c:161 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xf4/0x400 net/netfilter/core.c:626 nf_hook include/linux/netfilter.h:269 [inline] NF_HOOK include/linux/netfilter.h:312 [inline] ipv6_rcv+0x29b/0x390 net/ipv6/ip6_input.c:310 __netif_receive_skb_one_core ---truncated---			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: perf: Fix perf_pending_task() UaF Per syzbot it is possible for perf_pending_task() to run after the event is free()'d. There are two related but distinct cases: - the task_work was already queued before destroying the event; - destroying the event itself queues the task_work. The first cannot be solved using task_work_cancel() since perf_release() itself might be called from a task_work (____fput), which means the current->task_works list is already empty and task_work_cancel() won't be able to find the perf_pending_task() entry. The simplest alternative is extending the perf_event lifetime to cover the task_work. The second is just silly, queueing a task_work while you know the event is going away makes no sense and is easily avoided by re-arranging how the event is marked STATE_DEAD and ensuring it goes through STATE_OFF on the way down.	2024-10-21	7.8	CVE-2022-48950
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ASoC: ops: Check bounds for second channel in snd_soc_put_volsw_sx() The bounds checks in snd_soc_put_volsw_sx() are only being applied to the first channel, meaning it is possible to write out of bounds values to the second channel in stereo controls. Add appropriate checks.	2024-10-21	7.8	CVE-2022-48951
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: s390/qeth: fix use-after-free in hsci KASAN found that addr was dereferenced after br2dev_event_work was freed. == BUG: KASAN: use-after-free in qeth_l2_br2dev_worker+0x5ba/0x6b0 Read of size 1 at addr 00000000fdcea440 by task kworker/u760:4/540 CPU: 17 PID: 540	2024-10-21	7.8	CVE-2022-48954

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Comm: kworker/u760:4 Tainted: G E 6.1.0-20221128.rc7.git1.5aa3bed4ce83.300.fc36.s390x+kasan #1 Hardware name: IBM 8561 T01 703 (LPAR) Workqueue: 0.0.8000_event qeth_l2_br2dev_worker Call Trace: [<000000016944d4ce>] dump_stack_lvl+0xc6/0xf8 [<000000016942cd9c>] print_address_description.constprop.0+0x34/0x2a0 [<000000016942d118>] print_report+0x110/0x1f8 [<0000000167a7bd04>] kasan_report+0xfc/0x128 [<000000016938d79a>] qeth_l2_br2dev_worker+0x5ba/0x6b0 [<00000001673edd1e>] process_one_work+0x76e/0x1128 [<00000001673ee85c>] worker_thread+0x184/0x1098 [<000000016740718a>] kthread+0x26a/0x310 [<00000001672c606a>] __ret_from_fork+0x8a/0xe8 [<00000001694711da>] ret_from_fork+0xa/0x40 Allocated by task 108338: kasan_save_stack+0x40/0x68 kasan_set_track+0x36/0x48 __kasan_kmalloc+0xa0/0xc0 qeth_l2_switchdev_event+0x25a/0x738 atomic_notifier_call_chain+0x9c/0xf8 br_switchdev_fdb_notify+0xf4/0x110 fdb_notify+0x122/0x180 fdb_add_entry.constprop.0.isra.0+0x312/0x558 br_fdb_add+0x59e/0x858 rtnl_fdb_add+0x58a/0x928 rtnetlink_rcv_msg+0x5f8/0x8d8 netlink_rcv_skb+0x1f2/0x408 netlink_unicast+0x570/0x790 netlink_sendmsg+0x752/0xbe0 sock_sendmsg+0xca/0x110 ____sys_sendmsg+0x510/0x6a8 ___sys_sendmsg+0x12a/0x180 __sys_sendmsg+0xe6/0x168 __do_sys_socketcall+0x3c8/0x468 do_syscall+0x22c/0x328 __do_syscall+0x94/0xf0 system_call+0x82/0xb0 Freed by task 540: kasan_save_stack+0x40/0x68 kasan_set_track+0x36/0x48 kasan_save_free_info+0x4c/0x68 ____kasan_slab_free+0x14e/0x1a8 __kasan_slab_free+0x24/0x30 __kmem_cache_free+0x168/0x338 qeth_l2_br2dev_worker+0x154/0x6b0 process_one_work+0x76e/0x1128 worker_thread+0x184/0x1098 kthread+0x26a/0x310 __ret_from_fork+0x8a/0xe8 ret_from_fork+0xa/0x40 Last potentially related work creation: kasan_save_stack+0x40/0x68 __kasan_record_aux_stack+0xbe/0xd0 insert_work+0x56/0x2e8 __queue_work+0x4ce/0xd10 queue_work_on+0xf4/0x100 qeth_l2_switchdev_event+0x520/0x738 atomic_notifier_call_chain+0x9c/0xf8 br_switchdev_fdb_notify+0xf4/0x110 fdb_notify+0x122/0x180 fdb_add_entry.constprop.0.isra.0+0x312/0x558 br_fdb_add+0x59e/0x858 rtnl_fdb_add+0x58a/0x928 rtnetlink_rcv_msg+0x5f8/0x8d8 netlink_rcv_skb+0x1f2/0x408 netlink_unicast+0x570/0x790 netlink_sendmsg+0x752/0xbe0 sock_sendmsg+0xca/0x110 ____sys_sendmsg+0x510/0x6a8 ___sys_sendmsg+0x12a/0x180 __sys_sendmsg+0xe6/0x168 __do_sys_socketcall+0x3c8/0x468 do_syscall+0x22c/0x328 __do_syscall+0x94/0xf0 system_call+0x82/0xb0 Second to last potentially related work creation: kasan_save_stack+0x40/0x68 __kasan_record_aux_stack+0xbe/0xd0 kvfree_call_rcu+0xb2/0x760 kernfs_unlink_open_file+0x348/0x430 kernfs_fop_release+0xc2/0x320 __fput+0x1ae/0x768 task_work_run+0x1bc/0x298 exit_to_user_mode_prepare+0x1a0/0x1a8 __do_syscall+0x94/0xf0 system_call+0x82/0xb0 The buggy address belongs to the object at 00000000fdcea400 which belongs to the cache kmalloc-96 of size 96 The buggy address is located 64 bytes inside of 96-byte region [00000000fdcea400, 00000000fdcea460) The buggy address belongs to the physical page: page:000000005a9c26e8 refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0xfdcea flags: 0x3ffff00000000200(slab|node=0|zone=1|lastcpupid=0x1ffff) raw: 3ffff00000000200 0000000000000000 0000000100000122 000000008008cc00 raw: 0000000000000000 0020004100000000 ffffffff00000001 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: 00000000fdcea300: fb fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc 00000000fdcea380: fb fb fb fb fb fb f ---truncated---				

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ipv6: avoid use-after-free in ip6_fragment() Blamed commit claimed rcu_read_lock() was held by ip6_fragment() callers. It seems to not be always true, at least for UDP stack. syzbot reported: BUG: KASAN: use-after-free in ip6_dst_idev include/net/ip6_fib.h:245 [inline] BUG: KASAN: use-after-free in ip6_fragment+0x2724/0x2770 net/ipv6/ip6_output.c:951 Read of size 8 at addr ffff88801d403e80 by task syz-executor.3/7618 CPU: 1 PID: 7618 Comm: syz-executor.3 Not tainted 6.1.0-rc6-syzkaller-00012-g4312098baf37 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/26/2022 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xd1/0x138 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:284 [inline] print_report+0x15e/0x45d mm/kasan/report.c:395 kasan_report+0xbf/0x1f0 mm/kasan/report.c:495 ip6_dst_idev include/net/ip6_fib.h:245 [inline] ip6_fragment+0x2724/0x2770 net/ipv6/ip6_output.c:951 __ip6_finish_output net/ipv6/ip6_output.c:193 [inline] ip6_finish_output+0x9a3/0x1170 net/ipv6/ip6_output.c:206 NF_HOOK_COND include/linux/netfilter.h:291 [inline] ip6_output+0x1f1/0x540 net/ipv6/ip6_output.c:227 dst_output include/net/dst.h:445 [inline] ip6_local_out+0xb3/0x1a0 net/ipv6/output_core.c:161 ip6_send_skb+0xbb/0x340 net/ipv6/ip6_output.c:1966 udp_v6_send_skb+0x82a/0x18a0 net/ipv6/udp.c:1286 udp_v6_push_pending_frames+0x140/0x200 net/ipv6/udp.c:1313 udpv6_sendmsg+0x18da/0x2c80 net/ipv6/udp.c:1606 inet6_sendmsg+0x9d/0xe0 net/ipv6/af_inet6.c:665 sock_sendmsg_nosec net/socket.c:714 [inline] sock_sendmsg+0xd3/0x120 net/socket.c:734 sock_write_iter+0x295/0x3d0 net/socket.c:1108 call_write_iter include/linux/fs.h:2191 [inline] new_sync_write fs/read_write.c:491 [inline] vfs_write+0x9ed/0xdd0 fs/read_write.c:584 ksys_write+0x1ec/0x250 fs/read_write.c:637 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x39/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7fde3588c0d9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 f1 19 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fde365b6168 EFLAGS: 00000246 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 00007fde359ac050 RCX: 00007fde3588c0d9 RDX: 000000000000ffdc RSI: 00000000200000c0 RDI: 000000000000000a RBP: 00007fde358e7ae9 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007fde35acfb1f R14: 00007fde365b6300 R15: 0000000000022000 </TASK> Allocated by task 7618: kasan_save_stack+0x22/0x40 mm/kasan/common.c:45 kasan_set_track+0x25/0x30 mm/kasan/common.c:52 __kasan_slab_alloc+0x82/0x90 mm/kasan/common.c:325 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slab.h:737 [inline] slab_alloc_node mm/slub.c:3398 [inline] slab_alloc mm/slub.c:3406 [inline] __kmem_cache_alloc_lru mm/slub.c:3413 [inline] kmem_cache_alloc+0x2b4/0x3d0 mm/slub.c:3422 dst_alloc+0x14a/0x1f0 net/core/dst.c:92 ip6_dst_alloc+0x32/0xa0 net/ipv6/route.c:344 ip6_rt_pcpu_alloc net/ipv6/route.c:1369 [inline] rt6_make_pcpu_route net/ipv6/route.c:1417 [inline] ip6_pol_route+0x901/0x1190 net/ipv6/route.c:2254 pol_lookup_func include/net/ip6_fib.h:582 [inline] fib6_rule_lookup+0x52e/0x6f0 net/ipv6/fib6_rules.c:121 ip6_route_output_flags_noref+0x2e6/0x380 net/ipv6/route.c:2625 ip6_route_output_flags+0x76/0x320 net/ipv6/route.c:2638 ip6_route_output include/net/ip6_route.h:98 [inline] ip6_dst_lookup_tail+0x5ab/0x1620 net/ipv6/ip6_output.c:1092 ip6_dst_lookup_flow+0x90/0x1d0 net/ipv6/ip6_output.c:1222 ip6_sk_dst_lookup_flow+0x553/0x980 net/ipv6/ip6_output.c:1260 udpv6_sendmsg+0x151d/0x2c80 net/ipv6/udp.c:1554 inet6_sendmsg+0x9d/0xe0 net/ipv6/af_inet6.c:665 sock_sendmsg_nosec n ---truncated---	2024-10-21	7.8	CVE-2022-48956

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: hisilicon: Fix potential use-after-free in hix5hd2_rx() The skb is delivered to napi_gro_receive() which may free it, after calling this, dereferencing skb may trigger use-after-free.	2024-10-21	7.8	CVE-2022-48960
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: hisilicon: Fix potential use-after-free in hisi_femac_rx() The skb is delivered to napi_gro_receive() which may free it, after calling this, dereferencing skb may trigger use-after-free.	2024-10-21	7.8	CVE-2022-48962
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ravb: Fix potential use-after-free in ravb_rx_gbeth() The skb is delivered to napi_gro_receive() which may free it, after calling this, dereferencing skb may trigger use-after-free.	2024-10-21	7.8	CVE-2022-48964
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: mvneta: Prevent out of bounds read in mvneta_config_rss() The pp->indir[0] value comes from the user. It is passed to: if (cpu_online(pp->rxq_def)) inside the mvneta_percpu_elect() function. It needs bounds checkeding to ensure that it is not beyond the end of the cpu bitmap.	2024-10-21	7.1	CVE-2022-48966
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: NFC: nci: Bounds check struct nfc_target arrays While running under CONFIG_FORTIFY_SOURCE=y, syzkaller reported: memcpy: detected field-spanning write (size 129) of single field "target->sensf_res" at net/nfc/nci/ntf.c:260 (size 18) This appears to be a legitimate lack of bounds checking in nci_add_new_protocol(). Add the missing checks.	2024-10-21	7.1	CVE-2022-48967
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: dsa: sja1105: avoid out of bounds access in sja1105_init_l2_policing() The SJA1105 family has 45 L2 policing table entries (SJA1105_MAX_L2_POLICING_COUNT) and SJA1110 has 110 (SJA1110_MAX_L2_POLICING_COUNT). Keeping the table structure but accounting for the difference in port count (5 in SJA1105 vs 10 in SJA1110) does not fully explain the difference. Rather, the SJA1110 also has L2 ingress policers for multicast traffic. If a packet is classified as multicast, it will be processed by the policer index 99 + SRCPORT. The sja1105_init_l2_policing() function initializes all L2 policers such that they don't interfere with normal packet reception by default. To have a common code between SJA1105 and SJA1110, the index of the multicast policer for the port is calculated because it's an index that is out of bounds for SJA1105 but in bounds for SJA1110, and a bounds check is performed. The code fails to do the proper thing when determining what to do with the multicast policer of port 0 on SJA1105 (ds->num_ports = 5). The "mcast" index will be equal to 45, which is also equal to table->ops->max_entry_count (SJA1105_MAX_L2_POLICING_COUNT). So it passes through the check. But at the same time, SJA1105 doesn't have multicast policers. So the code programs the SHARINDX field of an out-of-bounds element in the L2 Policing table of the static config. The comparison between index 45 and 45 entries should have determined the code to not access this policer index on SJA1105, since its memory wasn't even allocated. With enough bad luck, the out-of-bounds write could even overwrite other valid kernel data, but in this case, the issue was detected using KASAN. Kernel log: sja1105 spi5.0: Probed switch chip: SJA1105Q == BUG: KASAN: slab-out-of-bounds in sja1105_setup+0x1cbc/0x2340 Write of size 8 at addr ffffff880bd57708 by task kworker/u8:0/8 ... Workqueue: events_unbound deferred_probe_work_func Call trace: ... sja1105_setup+0x1cbc/0x2340 dsa_register_switch+0x1284/0x18d0 sja1105_probe+0x748/0x840 ... Allocated by task 8: ... sja1105_setup+0x1bcc/0x2340 dsa_register_switch+0x1284/0x18d0 sja1105_probe+0x748/0x840 ...	2024-10-21	7.8	CVE-2022-48980

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/shmem-helper: Remove errant put in error path drm_gem_shmem_mmap() doesn't own this reference, resulting in the GEM object getting prematurely freed leading to a later use-after-free.	2024-10-21	7.8	CVE-2022-48981
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix use-after-free during gpu recovery [Why] [754.862560] refcount_t: underflow; use-after-free. [754.862898] Call Trace: [754.862903] <TASK> [754.862913] amdgpu_job_free_cb+0xc2/0xe1 [amdgpu] [754.863543] drm_sched_main.cold+0x34/0x39 [amd_sched] [How] The fw_fence may be not init, check whether dma_fence_init is performed before job free	2024-10-21	7.8	CVE-2022-48990
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: tracing: Free buffers when a used dynamic event is removed After 65536 dynamic events have been added and removed, the "type" field of the event then uses the first type number that is available (not currently used by other events). A type number is the identifier of the binary blobs in the tracing ring buffer (known as events) to map them to logic that can parse the binary blob. The issue is that if a dynamic event (like a kprobe event) is traced and is in the ring buffer, and then that event is removed (because it is dynamic, which means it can be created and destroyed), if another dynamic event is created that has the same number that new event's logic on parsing the binary blob will be used. To show how this can be an issue, the following can crash the kernel: # cd /sys/kernel/tracing # for i in `seq 65536`; do echo 'p:kprobes/foo do_sys_openat2 $arg1:u32' > kprobe_events # done For every iteration of the above, the writing to the kprobe_events will remove the old event and create a new one (with the same format) and increase the type number to the next available on until the type number reaches over 65535 which is the max number for the 16 bit type. After it reaches that number, the logic to allocate a new number simply looks for the next available number. When an dynamic event is removed, that number is then available to be reused by the next dynamic event created. That is, once the above reaches the max number, the number assigned to the event in that loop will remain the same. Now that means deleting one dynamic event and created another will reuse the previous events type number. This is where bad things can happen. After the above loop finishes, the kprobes/foo event which reads the do_sys_openat2 function call's first parameter as an integer. # echo 1 > kprobes/foo/enable # cat /etc/passwd > /dev/null # cat trace cat-2211 [005] .... 2007.849603: foo: (do_sys_openat2+0x0/0x130) arg1=4294967196 cat-2211 [005] .... 2007.849620: foo: (do_sys_openat2+0x0/0x130) arg1=4294967196 cat-2211 [005] .... 2007.849838: foo: (do_sys_openat2+0x0/0x130) arg1=4294967196 cat-2211 [005] .... 2007.849880: foo: (do_sys_openat2+0x0/0x130) arg1=4294967196 # echo 0 > kprobes/foo/enable Now if we delete the kprobe and create a new one that reads a string: # echo 'p:kprobes/foo do_sys_openat2 +0($arg2):string' > kprobe_events And now we can the trace: # cat trace sendmail-1942 [002] ..... 530.136320: foo: (do_sys_openat2+0x0/0x240) arg1= cat-2046 [004] ..... 530.930817: foo: (do_sys_openat2+0x0/0x240) arg1="??" cat-2046 [004] ..... 530.930961: foo: (do_sys_openat2+0x0/0x240) arg1="??" cat-2046 [004] ..... 530.934278: foo: (do_sys_openat2+0x0/0x240) arg1="??" cat-2046 [004] ..... 530.934563: foo: (do_sys_openat2+0x0/0x240) arg1="??????????????????????????????????????? ---truncated---	2024-10-21	7.8	CVE-2022-49006
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: tun: Fix use-after-free in tun_detach() syzbot reported use-after-free in tun_detach() [1]. This causes call trace like below: ==	2024-10-21	7.8	CVE-2022-49014

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	BUG: KASAN: use-after-free in notifier_call_chain+0x1ee/0x200 kernel/notifier.c:75 Read of size 8 at addr ffff88807324e2a8 by task syz-executor.0/3673 CPU: 0 PID: 3673 Comm: syz-executor.0 Not tainted 6.1.0-rc5-syzkaller-00044-gcc675d22e422 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/26/2022 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xd1/0x138 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:284 [inline] print_report+0x15e/0x461 mm/kasan/report.c:395 kasan_report+0xbf/0x1f0 mm/kasan/report.c:495 notifier_call_chain+0x1ee/0x200 kernel/notifier.c:75 call_netdevice_notifiers_info+0x86/0x130 net/core/dev.c:1942 call_netdevice_notifiers_extack net/core/dev.c:1983 [inline] call_netdevice_notifiers net/core/dev.c:1997 [inline] netdev_wait_allrefs_any net/core/dev.c:10237 [inline] netdev_run_todo+0xbc6/0x1100 net/core/dev.c:10351 tun_detach drivers/net/tun.c:704 [inline] tun_chr_close+0xe4/0x190 drivers/net/tun.c:3467 __fput+0x27c/0xa90 fs/file_table.c:320 task_work_run+0x16f/0x270 kernel/task_work.c:179 exit_task_work include/linux/task_work.h:38 [inline] do_exit+0xb3d/0x2a30 kernel/exit.c:820 do_group_exit+0xd4/0x2a0 kernel/exit.c:950 get_signal+0x21b1/0x2440 kernel/signal.c:2858 arch_do_signal_or_restart+0x86/0x2300 arch/x86/kernel/signal.c:869 exit_to_user_mode_loop kernel/entry/common.c:168 [inline] exit_to_user_mode_prepare+0x15f/0x250 kernel/entry/common.c:203 __syscall_exit_to_user_mode_work kernel/entry/common.c:285 [inline] syscall_exit_to_user_mode+0x1d/0x50 kernel/entry/common.c:296 do_syscall_64+0x46/0xb0 arch/x86/entry/common.c:86 entry_SYSCALL_64_after_hwframe+0x63/0xcd The cause of the issue is that sock_put() from __tun_detach() drops last reference count for struct net, and then notifier_call_chain() from netdev_state_change() accesses that struct net. This patch fixes the issue by calling sock_put() from tun_detach() after all necessary accesses for the struct net has done.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: hsr: Fix potential use-after-free The skb is delivered to netif_rx() which may free it, after calling this, dereferencing skb may trigger use-after-free.	2024-10-21	7.8	CVE-2022-49015
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: tipc: re-fetch skb cb after tipc_msg_validate As the call trace shows, the original skb was freed in tipc_msg_validate(), and dereferencing the old skb cb would cause an use-after-free crash. BUG: KASAN: use-after-free in tipc_crypto_rcv_complete+0x1835/0x2240 [tipc] Call Trace: <IRQ> tipc_crypto_rcv_complete+0x1835/0x2240 [tipc] tipc_crypto_rcv+0xd32/0x1ec0 [tipc] tipc_rcv+0x744/0x1150 [tipc] ... Allocated by task 47078: kmem_cache_alloc_node+0x158/0x4d0 __alloc_skb+0x1c1/0x270 tipc_buf_acquire+0x1e/0xe0 [tipc] tipc_msg_create+0x33/0x1c0 [tipc] tipc_link_build_proto_msg+0x38a/0x2100 [tipc] tipc_link_timeout+0x8b8/0xef0 [tipc] tipc_node_timeout+0x2a1/0x960 [tipc] call_timer_fn+0x2d/0x1c0 ... Freed by task 47078: tipc_msg_validate+0x7b/0x440 [tipc] tipc_crypto_rcv_complete+0x4b5/0x2240 [tipc] tipc_crypto_rcv+0xd32/0x1ec0 [tipc] tipc_rcv+0x744/0x1150 [tipc] This patch fixes it by re-fetching the skb cb from the new allocated skb after calling tipc_msg_validate().	2024-10-21	7.8	CVE-2022-49017
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: mac8021: fix possible oob access in ieee80211_get_rate_duration Fix possible out-of-bound access in ieee80211_get_rate_duration routine as reported by the following UBSAN report: UBSAN: array-index-out-of-bounds in net/mac80211/airtime.c:455:47 index 15 is out of range for type 'u16 [12]' CPU: 2 PID: 217 Comm: kworker/u32:10 Not tainted 6.1.0-060100rc3-generic Hardware name: Acer Aspire TC-281/Aspire TC-281, BIOS R01-A2 07/18/2017 Workqueue: mt76 mt76u_tx_status_data [mt76_usb] Call Trace: <TASK> show_stack+0x4e/0x61 dump_stack_lvl+0x4a/0x6f dump_stack+0x10/0x18 ubsan_epilogue+0x9/0x43 __ubsan_handle_out_of_bounds.cold+0x42/0x47	2024-10-21	7.8	CVE-2022-49022

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ieee80211_get_rate_duration.constprop.0+0x22f/0x2a0 [mac80211] ? ieee80211_tx_status_ext+0x32e/0x640 [mac80211] ieee80211_calc_rx_airtime+0xda/0x120 [mac80211] ieee80211_calc_tx_airtime+0xb4/0x100 [mac80211] mt76x02_send_tx_status+0x266/0x480 [mt76x02_lib] mt76x02_tx_status_data+0x52/0x80 [mt76x02_lib] mt76u_tx_status_data+0x67/0xd0 [mt76_usb] process_one_work+0x225/0x400 worker_thread+0x50/0x3e0 ? process_one_work+0x400/0x400 kthread+0xe9/0x110 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork+0x22/0x30			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: fix buffer overflow in elem comparison For vendor elements, the code here assumes that 5 octets are present without checking. Since the element itself is already checked to fit, we only need to check the length.	2024-10-21	7.8	CVE-2022-49023
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix use-after-free when reverting termination table When having multiple dests with termination tables and second one or afterwards fails the driver reverts usage of term tables but doesn't reset the assignment in attr->dests[num_vport_dests].termtbl which case a use-after-free when releasing the rule. Fix by resetting the assignment of termtbl to null.	2024-10-21	7.8	CVE-2022-49025
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: e100: Fix possible use after free in e100_xmit_prepare In e100_xmit_prepare(), if we can't map the skb, then return -ENOMEM, so e100_xmit_frame() will return NETDEV_TX_BUSY and the upper layer will resend the skb. But the skb is already freed, which will cause UAF bug when the upper layer resends the skb. Remove the harmful free.	2024-10-21	7.8	CVE-2022-49026
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: hwmon: (ibmpex) Fix possible UAF when ibmpex_register_bmc() fails Smatch report warning as follows: drivers/hwmon/ibmpex.c:509 ibmpex_register_bmc() warn: '&data->list' not removed from list If ibmpex_find_sensors() fails in ibmpex_register_bmc(), data will be freed, but data->list will not be removed from driver_data.bmc_data, then list traversal may cause UAF. Fix by removeing it from driver_data.bmc_data before free().	2024-10-21	7.8	CVE-2022-49029
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: libbpf: Handle size overflow for ringbuf mmap The maximum size of ringbuf is 2GB on x86-64 host, so 2 * max_entries will overflow u32 when mapping producer page and data pages. Only casting max_entries to size_t is not enough, because for 32-bits application on 64-bits kernel the size of read-only mmap region also could overflow size_t. So fixing it by casting the size of read-only mmap region into a __u64 and checking whether or not there will be overflow during mmap.	2024-10-21	7.8	CVE-2022-49030
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: iio: health: afe4403: Fix oob read in afe4403_read_raw KASAN report out-of-bounds read as follows: BUG: KASAN: global-out-of-bounds in afe4403_read_raw+0x42e/0x4c0 Read of size 4 at addr ffffffffc02ac638 by task cat/279 Call Trace: afe4403_read_raw iio_read_channel_info dev_attr_show The buggy address belongs to the variable: afe4403_channel_leds+0x18/0xffffffffffffe9e0 This issue can be reproduced by singe command: $ cat /sys/bus/spi/devices/spi0.0/iio\:device0/in_intensity6_raw The array size of afe4403_channel_leds is less than channels, so access with chan->address cause OOB read in afe4403_read_raw. Fix it by moving access before use it.	2024-10-21	7.1	CVE-2022-49031
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: iio: health: afe4404: Fix oob read in afe4404_[read|write]_raw KASAN report out-of-bounds read as follows: BUG: KASAN: global-out-of-bounds in afe4404_read_raw+0x2ce/0x380 Read of size 4 at addr ffffffffc00e4658 by task	2024-10-21	7.1	CVE-2022-49032

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cat/278 Call Trace: afe4404_read_raw iio_read_channel_info dev_attr_show The buggy address belongs to the variable: afe4404_channel_leds+0x18/0xffffffffffffe9c0 This issue can be reproduce by singe command: $ cat /sys/bus/i2c/devices/0-0058/iio\:device0/in_intensity6_raw The array size of afe4404_channel_leds and afe4404_channel_offdacs are less than channels, so access with chan->address cause OOB read in afe4404_[read|write]_raw. Fix it by moving access before use them.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix use-after-free in bpf_uprobe_multi_link_attach() If bpf_link_prime() fails, bpf_uprobe_multi_link_attach() goes to the error_free label and frees the array of bpf_uprobe's without calling bpf_uprobe_unregister(). This leaks bpf_uprobe->uprobe and worse, this frees bpf_uprobe->consumer without removing it from the uprobe->consumers list.	2024-10-21	7.8	CVE-2024-47675
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb.c: fix UAF of vma in hugetlb fault pathway Syzbot reports a UAF in hugetlb_fault(). This happens because vmf_anon_prepare() could drop the per-VMA lock and allow the current VMA to be freed before hugetlb_vma_unlock_read() is called. We can fix this by using a modified version of vmf_anon_prepare() that doesn't release the VMA lock on failure, and then release it ourselves after hugetlb_vma_unlock_read().	2024-10-21	7.8	CVE-2024-47676
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: scsi: sd: Fix off-by-one error in sd_read_block_characteristics() Ff the device returns page 0xb1 with length 8 (happens with qemu v2.x, for example), sd_read_block_characteristics() may attempt an out-of-bounds memory access when accessing the zoned field at offset 8.	2024-10-21	7.8	CVE-2024-47682
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ep93xx: clock: Fix off by one in ep93xx_div_recalc_rate() The psc->div[] array has psc->num_div elements. These values come from when we call clk_hw_register_div(). It's adc_divisors and ARRAY_SIZE(adc_divisors)) and so on. So this condition needs to be >= instead of > to prevent an out of bounds read.	2024-10-21	7.1	CVE-2024-47686
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid use-after-free in f2fs_stop_gc_thread() syzbot reports a f2fs bug as below: __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:114 print_report+0xe8/0x550 mm/kasan/report.c:491 kasan_report+0x143/0x180 mm/kasan/report.c:601 kasan_check_range+0x282/0x290 mm/kasan/generic.c:189 instrument_atomic_read_write include/linux/instrumented.h:96 [inline] atomic_fetch_add_relaxed include/linux/atomic/atomic-instrumented.h:252 [inline] __refcount_add include/linux/refcount.h:184 [inline] __refcount_inc include/linux/refcount.h:241 [inline] refcount_inc include/linux/refcount.h:258 [inline] get_task_struct include/linux/sched/task.h:118 [inline] kthread_stop+0xca/0x630 kernel/kthread.c:704 f2fs_stop_gc_thread+0x65/0xb0 fs/f2fs/gc.c:210 f2fs_do_shutdown+0x192/0x540 fs/f2fs/file.c:2283 f2fs_ioc_shutdown fs/f2fs/file.c:2325 [inline] __f2fs_ioctl+0x443a/0xbe60 fs/f2fs/file.c:4325 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl+0xfc/0x170 fs/ioctl.c:893 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f The root cause is below race condition, it may cause use-after-free issue in sbi->gc_th pointer. - remount - f2fs_remount - f2fs_stop_gc_thread - kfree(gc_th) - f2fs_ioc_shutdown - f2fs_do_shutdown - f2fs_stop_gc_thread - kthread_stop(gc_th->f2fs_gc_task) : sbi->gc_thread = NULL; We will call f2fs_do_shutdown() in two paths: - for f2fs_ioc_shutdown() path, we should grab	2024-10-21	7.8	CVE-2024-47691

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sb->s_umount semaphore for fixing. - for f2fs_shutdown() path, it's safe since caller has already grabbed sb->s_umount semaphore.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: RDMA/rtrs-clt: Reset cid to con_num - 1 to stay in bounds In the function init_conns(), after the create_con() and create_cm() for loop if something fails. In the cleanup for loop after the destroy tag, we access out of bound memory because cid is set to clt_path->s.con_num. This commits resets the cid to clt_path->s.con_num - 1, to stay in bounds in the cleanup loop later.	2024-10-21	7.8	CVE-2024-47695
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: RDMA/iwcm: Fix WARNING:at_kernel/workqueue.c:#check_flush_dependency In the commit aee2424246f9 ("RDMA/iwcm: Fix a use-after-free related to destroying CM IDs"), the function flush_workqueue is invoked to flush the work queue iwcm_wq. But at that time, the work queue iwcm_wq was created via the function alloc_ordered_workqueue without the flag WQ_MEM_RECLAIM. Because the current process is trying to flush the whole iwcm_wq, if iwcm_wq doesn't have the flag WQ_MEM_RECLAIM, verify that the current process is not reclaiming memory or running on a workqueue which doesn't have the flag WQ_MEM_RECLAIM as that can break forward-progress guarantee leading to a deadlock. The call trace is as below: [125.350876][T1430] Call Trace: [125.356281][T1430] <TASK> [125.361285][T1430] ? __warn (kernel/panic.c:693) [125.367640][T1430] ? check_flush_dependency (kernel/workqueue.c:3706 (discriminator 9)) [125.375689][T1430] ? report_bug (lib/bug.c:180 lib/bug.c:219) [125.382505][T1430] ? handle_bug (arch/x86/kernel/traps.c:239) [125.388987][T1430] ? exc_invalid_op (arch/x86/kernel/traps.c:260 (discriminator 1)) [125.395831][T1430] ? asm_exc_invalid_op (arch/x86/include/asm/idtentry.h:621) [125.403125][T1430] ? check_flush_dependency (kernel/workqueue.c:3706 (discriminator 9)) [125.410984][T1430] ? check_flush_dependency (kernel/workqueue.c:3706 (discriminator 9)) [125.418764][T1430] __flush_workqueue (kernel/workqueue.c:3970) [125.426021][T1430] ? __pfx___might_resched (kernel/sched/core.c:10151) [125.433431][T1430] ? destroy_cm_id (drivers/infiniband/core/iwcm.c:375) iw_cm [125.441209][T1430] ? __pfx___flush_workqueue (kernel/workqueue.c:3910) [125.473900][T1430] ? _raw_spin_lock_irqsave (arch/x86/include/asm/atomic.h:107 include/linux/atomic/atomic-arch-fallback.h:2170 include/linux/atomic/atomic-instrumented.h:1302 include/asm-generic/qspinlock.h:111 include/linux/spinlock.h:187 include/linux/spinlock_api_smp.h:111 kernel/locking/spinlock.c:162) [125.473909][T1430] ? __pfx__raw_spin_lock_irqsave (kernel/locking/spinlock.c:161) [125.482537][T1430] _destroy_id (drivers/infiniband/core/cma.c:2044) rdma_cm [125.495072][T1430] nvme_rdma_free_queue (drivers/nvme/host/rdma.c:656 drivers/nvme/host/rdma.c:650) nvme_rdma [125.505827][T1430] nvme_rdma_reset_ctrl_work (drivers/nvme/host/rdma.c:2180) nvme_rdma [125.505831][T1430] process_one_work (kernel/workqueue.c:3231) [125.515122][T1430] worker_thread (kernel/workqueue.c:3306 kernel/workqueue.c:3393) [125.515127][T1430] ? __pfx_worker_thread (kernel/workqueue.c:3339) [125.531837][T1430] kthread (kernel/kthread.c:389) [125.539864][T1430] ? __pfx_kthread (kernel/kthread.c:342) [125.550628][T1430] ret_from_fork (arch/x86/kernel/process.c:147) [125.558840][T1430] ? __pfx_kthread (kernel/kthread.c:342) [125.558844][T1430] ret_from_fork_asm (arch/x86/entry/entry_64.S:257) [125.566487][T1430] </TASK> [125.566488][T1430] ---[end trace 0000000000000000]---	2024-10-21	7.8	CVE-2024-47696
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drivers: media: dvb-frontends/rtl2830: fix an out-of-bounds write error Ensure index in rtl2830_pid_filter does not exceed 31 to prevent out-of-bounds access. dev->filters is a 32-bit value, so set_bit and clear_bit functions should only operate on indices from 0 to 31. If index is 32, it will attempt to access a non-existent 33rd bit,	2024-10-21	7.8	CVE-2024-47697

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	leading to out-of-bounds access. Change the boundary check from index > 32 to index >= 32 to resolve this issue.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drivers: media: dvb-frontends/rtl2832: fix an out-of-bounds write error Ensure index in rtl2832_pid_filter does not exceed 31 to prevent out-of-bounds access. dev->filters is a 32-bit value, so set_bit and clear_bit functions should only operate on indices from 0 to 31. If index is 32, it will attempt to access a non-existent 33rd bit, leading to out-of-bounds access. Change the boundary check from index > 32 to index >= 32 to resolve this issue. [hverkuil: added fixes tag, rtl2830_pid_filter -> rtl2832_pid_filter in logmsg]	2024-10-21	7.8	CVE-2024-47698
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ext4: avoid OOB when system.data xattr changes underneath the filesystem When looking up for an entry in an inlined directory, if e_value_offs is changed underneath the filesystem by some change in the block device, it will lead to an out-of-bounds access that KASAN detects as an UAF. EXT4-fs (loop0): mounted filesystem 00000000-0000-0000-0000-000000000000 r/w without journal. Quota mode: none. loop0: detected capacity change from 2048 to 2047 == BUG: KASAN: use-after-free in ext4_search_dir+0xf2/0x1c0 fs/ext4/namei.c:1500 Read of size 1 at addr ffff88803e91130f by task syz-executor269/5103 CPU: 0 UID: 0 PID: 5103 Comm: syz-executor269 Not tainted 6.11.0-rc4-syzkaller #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 ext4_search_dir+0xf2/0x1c0 fs/ext4/namei.c:1500 ext4_find_inline_entry+0x4be/0x5e0 fs/ext4/inline.c:1697 __ext4_find_entry+0x2b4/0x1b30 fs/ext4/namei.c:1573 ext4_lookup_entry fs/ext4/namei.c:1727 [inline] ext4_lookup+0x15f/0x750 fs/ext4/namei.c:1795 lookup_one_qstr_excl+0x11f/0x260 fs/namei.c:1633 filename_create+0x297/0x540 fs/namei.c:3980 do_symlinkat+0xf9/0x3a0 fs/namei.c:4587 __do_sys_symlinkat fs/namei.c:4610 [inline] __se_sys_symlinkat fs/namei.c:4607 [inline] __x64_sys_symlinkat+0x95/0xb0 fs/namei.c:4607 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f3e73ced469 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 21 18 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fff4d40c258 EFLAGS: 00000246 ORIG_RAX: 000000000000010a RAX: ffffffffffffffda RBX: 0032656c69662f2e RCX: 00007f3e73ced469 RDX: 0000000020000200 RSI: 00000000ffffff9c RDI: 0000000200001c0 RBP: 0000000000000000 R08: 00007fff4d40c290 R09: 00007fff4d40c290 R10: 0023706f6f6c2f76 R11: 0000000000000246 R12: 00007fff4d40c27c R13: 0000000000000003 R14: 431bde82d7b634db R15: 00007fff4d40c2b0 </TASK> Calling ext4_xattr_ibody_find right after reading the inode with ext4_get_inode_loc will lead to a check of the validity of the xattrs, avoiding this problem.	2024-10-21	7.8	CVE-2024-47701
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: af_unix: Don't return OOB skb in manage_oob(). syzbot reported use-after-free in unix_stream_recv_urg(). [0] The scenario is 1. send(MSG_OOB) 2. recv(MSG_OOB) -> The consumed OOB remains in recv queue 3. send(MSG_OOB) 4. recv() -> manage_oob() returns the next skb of the consumed OOB -> This is also OOB, but unix_sk(sk)->oob_skb is not cleared 5. recv(MSG_OOB) -> unix_sk(sk)->oob_skb is used but already freed The recent commit 8594d9b85c07 ("af_unix: Don't call skb_get() for OOB skb.") uncovered the issue. If the OOB skb is consumed and the next skb is peeked in manage_oob(), we still need to check if the skb is OOB. Let's do so by falling back to the following checks in manage_oob() and add the test	2024-10-21	7.8	CVE-2024-47711

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	case in selftest. Note that we need to add a similar check for SIOCATMARK. [0]: BUG: KASAN: slab-use-after-free in unix_stream_read_actor+0xa6/0xb0 net/unix/af_unix.c:2959 Read of size 4 at addr ffff8880326abcc4 by task syz-executor178/5235 CPU: 0 UID: 0 PID: 5235 Comm: syz-executor178 Not tainted 6.11.0-rc5-syzkaller-00742-gfbdaffe41adc #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 unix_stream_read_actor+0xa6/0xb0 net/unix/af_unix.c:2959 unix_stream_recv_urg+0x1df/0x320 net/unix/af_unix.c:2640 unix_stream_read_generic+0x2456/0x2520 net/unix/af_unix.c:2778 unix_stream_recvmsg+0x22b/0x2c0 net/unix/af_unix.c:2996 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x22f/0x280 net/socket.c:1068 ____sys_recvmsg+0x1db/0x470 net/socket.c:2816 ___sys_recvmsg net/socket.c:2858 [inline] __sys_recvmsg+0x2f0/0x3e0 net/socket.c:2888 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f5360d6b4e9 Code: 48 83 c4 28 c3 e8 37 17 00 00 0f 1f 80 00 00 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fff29b3a458 EFLAGS: 00000246 ORIG_RAX: 000000000000002f RAX: ffffffffffffffda RBX: 00007fff29b3a638 RCX: 00007f5360d6b4e9 RDX: 0000000000002001 RSI: 0000000020000640 RDI: 0000000000000003 RBP: 00007f5360dde610 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000001 R13: 00007fff29b3a628 R14: 0000000000000001 R15: 0000000000000001 </TASK> Allocated by task 5235: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:312 [inline] __kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_node_noprof+0x16b/0x320 mm/slub.c:4080 __alloc_skb+0x1c3/0x440 net/core/skbuff.c:667 alloc_skb include/linux/skbuff.h:1320 [inline] alloc_skb_with_frags+0xc3/0x770 net/core/skbuff.c:6528 sock_alloc_send_pskb+0x91a/0xa60 net/core/sock.c:2815 sock_alloc_send_skb include/net/sock.h:1778 [inline] queue_oob+0x108/0x680 net/unix/af_unix.c:2198 unix_stream_sendmsg+0xd24/0xf80 net/unix/af_unix.c:2351 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x221/0x270 net/socket.c:745 ____sys_sendmsg+0x525/0x7d0 net/socket.c:2597 ___sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 5235: kasan_save_stack mm/kasan/common.c:47 ---truncated---			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: always wait for both firmware loading attempts In 'rtw_wait_firmware_completion()', always wait for both (regular and wowlan) firmware loading attempts. Otherwise if 'rtw_usb_intf_init()' has failed in 'rtw_usb_probe()', 'rtw_usb_disconnect()' may issue 'ieee80211_free_hw()' when one of 'rtw_load_firmware_cb()' (usually the wowlan one) is still in progress, causing UAF detected by KASAN.	2024-10-21	7.8	CVE-2024-47718
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: iommufd: Protect against overflow of ALIGN() during iova allocation Userspace can supply an iova and uptr such that the target iova alignment becomes really big and ALIGN() overflows which corrupts the selected area range during allocation. CONFIG_IOMMUFD_TEST can detect this: WARNING: CPU: 1 PID: 5092 at drivers/iommu/iommufd/io_pagetable.c:268 iopt_alloc_area_pages	2024-10-21	7.8	CVE-2024-47719

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	drivers/iommu/iommufd/io_pagetable.c:268 [inline] WARNING: CPU: 1 PID: 5092 at drivers/iommu/iommufd/io_pagetable.c:268 iopt_map_pages+0xf95/0x1050 drivers/iommu/iommufd/io_pagetable.c:352 Modules linked in: CPU: 1 PID: 5092 Comm: syz-executor294 Not tainted 6.10.0-rc5-syzkaller-00294-g3ffea9a7a6f7 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/07/2024 RIP: 0010:iopt_alloc_area_pages drivers/iommu/iommufd/io_pagetable.c:268 [inline] RIP: 0010:iopt_map_pages+0xf95/0x1050 drivers/iommu/iommufd/io_pagetable.c:352 Code: fc e9 a4 f3 ff ff e8 1a 8b 4c fc 41 be e4 ff ff ff e9 8a f3 ff ff e8 0a 8b 4c fc 90 0f 0b 90 e9 37 f5 ff ff e8 fc 8a 4c fc 90 <0f> 0b 90 e9 68 f3 ff ff 48 c7 c1 ec 82 ad 8f 80 e1 07 80 c1 03 38 RSP: 0018:ffffc90003ebf9e0 EFLAGS: 00010293 RAX: ffffffff85499fa4 RBX: 00000000ffffffef RCX: ffff888079b49e00 RDX: 0000000000000000 RSI: 00000000ffffffef RDI: 0000000000000000 RBP: ffffc90003ebfc50 R08: ffffffff85499b30 R09: ffffffff85499942 R10: 0000000000000002 R11: ffff888079b49e00 R12: ffff8880228e0010 R13: 0000000000000000 R14: 1ffff920007d7f68 R15: ffffc90003ebfd00 FS: 000055557d760380(0000) GS:ffff8880b9500000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000005fdeb8 CR3: 000000007404a000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> iommufd_ioas_copy+0x610/0x7b0 drivers/iommu/iommufd/ioas.c:274 iommufd_fops_ioctl+0x4d9/0x5a0 drivers/iommu/iommufd/main.c:421 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl+0xfc/0x170 fs/ioctl.c:893 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Cap the automatic alignment to the huge page size, which is probably a better idea overall. Huge automatic alignments can fragment and chew up the available IOVA space without any reason.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: remove unused C2H event ID RTW89_MAC_C2H_FUNC_READ_WOW_CAM to prevent out-of-bounds reading The handler of firmware C2H event RTW89_MAC_C2H_FUNC_READ_WOW_CAM isn't implemented, but driver expects number of handlers is NUM_OF_RTW89_MAC_C2H_FUNC_WOW causing out-of-bounds access. Fix it by removing ID. Addresses-Coverity-ID: 1598775 ("Out-of-bounds read")	2024-10-21	7.1	CVE-2024-47721
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: jfs: fix out-of-bounds in dbNextAG() and diAlloc() In dbNextAG() , there is no check for the case where bmp->db_numag is greater or same than MAXAG due to a polluted image, which causes an out-of-bounds. Therefore, a bounds check should be added in dbMount(). And in dbNextAG(), a check for the case where agpref is greater than bmp->db_numag should be added, so an out-of-bounds exception should be prevented. Additionally, a check for the case where agno is greater or same than MAXAG should be added in diAlloc() to prevent out-of-bounds.	2024-10-21	7.1	CVE-2024-47723
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: x86/tdx: Fix "in-kernel MMIO" check TDX only supports kernel-initiated MMIO operations. The handle_mmio() function checks if the #VE exception occurred in the kernel and rejects the operation if it did not. However, userspace can deceive the kernel into performing MMIO on its behalf. For example, if userspace can point a syscall to an MMIO address, syscall does get_user() or put_user() on it, triggering MMIO #VE. The kernel will treat the #VE as in-kernel MMIO. Ensure that the target MMIO address is within the kernel before decoding instruction.	2024-10-21	7.8	CVE-2024-47727
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/qm - inject error before stopping queue The master ooo cannot be completely closed when the accelerator core reports memory error. Therefore, the driver needs to inject the qm error to close the master ooo. Currently, the qm	2024-10-21	7.8	CVE-2024-47730

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	error is injected after stopping queue, memory may be released immediately after stopping queue, causing the device to access the released memory. Therefore, error is injected to close master ooo before stopping queue to ensure that the device does not access the released memory.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: crypto: iaa - Fix potential use after free bug The free_device_compression_mode(iaa_device, device_mode) function frees "device_mode" but it iss passed to iaa_compression_modes[i]->free() a few lines later resulting in a use after free. The good news is that, so far as I can tell, nothing implements the ->free() function and the use after free happens in dead code. But, with this fix, when something does implement it, we'll be ready. :)	2024-10-21	7.8	CVE-2024-47732
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix race setting file private on concurrent lseek using same fd When doing concurrent lseek(2) system calls against the same file descriptor, using multiple threads belonging to the same process, we have a short time window where a race happens and can result in a memory leak. The race happens like this: 1) A program opens a file descriptor for a file and then spawns two threads (with the pthreads library for example), lets call them task A and task B; 2) Task A calls lseek with SEEK_DATA or SEEK_HOLE and ends up at file.c:find_desired_extent() while holding a read lock on the inode; 3) At the start of find_desired_extent(), it extracts the file's private_data pointer into a local variable named 'private', which has a value of NULL; 4) Task B also calls lseek with SEEK_DATA or SEEK_HOLE, locks the inode in shared mode and enters file.c:find_desired_extent(), where it also extracts file->private_data into its local variable 'private', which has a NULL value; 5) Because it saw a NULL file private, task A allocates a private structure and assigns to the file structure; 6) Task B also saw a NULL file private so it also allocates its own file private and then assigns it to the same file structure, since both tasks are using the same file descriptor. At this point we leak the private structure allocated by task A. Besides the memory leak, there's also the detail that both tasks end up using the same cached state record in the private structure (struct btrfs_file_private::llseek_cached_state), which can result in a use-after-free problem since one task can free it while the other is still using it (only one task took a reference count on it). Also, sharing the cached state is not a good idea since it could result in incorrect results in the future - right now it should not be a problem because it end ups being used only in extent-io-tree.c:count_range_bits() where we do range validation before using the cached state. Fix this by protecting the private assignment and check of a file while holding the inode's spinlock and keep track of the task that allocated the private, so that it's used only by that task in order to prevent user-after-free issues with the cached state record as well as potentially using it incorrectly in the future.	2024-10-21	7	CVE-2024-47741
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: firmware_loader: Block path traversal Most firmware names are hardcoded strings, or are constructed from fairly constrained format strings where the dynamic parts are just some hex numbers or such. However, there are a couple codepaths in the kernel where firmware file names contain string components that are passed through from a device or semi-privileged userspace; the ones I could find (not counting interfaces that require root privileges) are: - lpfc_sli4_request_firmware_update() seems to construct the firmware filename from "ModelName", a string that was previously parsed out of some descriptor ("Vital Product Data") in lpfc_fill_vpd() - nfp_net_fw_find() seems to construct a firmware filename from a model name coming from nfp_hwinfo_lookup(pf->hwinfo, "nffw.partno"), which I think parses some descriptor that was read from the device. (But this case likely isn't exploitable because the format string looks like "netronome/nic_%s", and there shouldn't be any *folders* starting with "netronome/nic_". The previous case was different because there, the "%s" is *at the start* of the format string.) - module_flash_fw_schedule() is reachable from the ETHTOOL_MSG_MODULE_FW_FLASH_ACT netlink command, which is marked as GENL_UNS_ADMIN_PERM (meaning CAP_NET_ADMIN inside a user namespace	2024-10-21	7.8	CVE-2024-47742

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is enough to pass the privilege check), and takes a userspace-provided firmware name. (But I think to reach this case, you need to have CAP_NET_ADMIN over a network namespace that a special kind of ethernet device is mapped into, so I think this is not a viable attack path in practice.) Fix it by rejecting any firmware names containing ".." path components. For what it's worth, I went looking and haven't found any USB device drivers that use the firmware loader dangerously.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: mm: call the security_mmap_file() LSM hook in remap_file_pages() The remap_file_pages syscall handler calls do_mmap() directly, which doesn't contain the LSM security check. And if the process has called personality(READ_IMPLIES_EXEC) before and remap_file_pages() is called for RW pages, this will actually result in remapping the pages to RWX, bypassing a W^X policy enforced by SELinux. So we should check prot by security_mmap_file LSM hook in the remap_file_pages syscall handler before do_mmap() is called. Otherwise, it potentially permits an attacker to bypass a W^X policy enforced by SELinux. The bypass is similar to CVE-2016-10044, which bypass the same thing via AIO and can be found in [1]. The PoC: $ cat > test.c int main(void) { size_t pagesz = sysconf(_SC_PAGE_SIZE); int mfd = syscall(SYS_memfd_create, "test", 0); const char *buf = mmap(NULL, 4 * pagesz, PROT_READ | PROT_WRITE, MAP_SHARED, mfd, 0); unsigned int old = syscall(SYS_personality, 0xffffffff); syscall(SYS_personality, READ_IMPLIES_EXEC | old); syscall(SYS_remap_file_pages, buf, pagesz, 0, 2, 0); syscall(SYS_personality, old); // show the RWX page exists even if W^X policy is enforced int fd = open("/proc/self/maps", O_RDONLY); unsigned char buf2[1024]; while (1) { int ret = read(fd, buf2, 1024); if (ret <= 0) break; write(1, buf2, ret); } close(fd); } $ gcc test.c -o test $ ./test | grep rwx 7f1836c34000-7f1836c35000 rwxs 00002000 00:01 2050 /memfd:test (deleted) [PM: subject line tweaks]	2024-10-21	7.8	CVE-2024-47745
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: seeq: Fix use after free vulnerability in ether3 Driver Due to Race Condition In the ether3_probe function, a timer is initialized with a callback function ether3_ledoff, bound to &prev(dev)->timer. Once the timer is started, there is a risk of a race condition if the module or device is removed, triggering the ether3_remove function to perform cleanup. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | ether3_ledoff ether3_remove | free_netdev(dev); | put_devic | kfree(dev); | | ether3_outw(priv(dev)->regs.config2 |= CFG2_CTRLO, REG_CONFIG2); | // use dev Fix it by ensuring that the timer is canceled before proceeding with the cleanup in ether3_remove.	2024-10-21	7	CVE-2024-47747
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: vhost_vdpa: assign irq bypass producer token correctly We used to call irq_bypass_unregister_producer() in vhost_vdpa_setup_vq_irq() which is problematic as we don't know if the token pointer is still valid or not. Actually, we use the eventfd_ctx as the token so the life cycle of the token should be bound to the VHOST_SET_VRING_CALL instead of vhost_vdpa_setup_vq_irq() which could be called by set_status(). Fixing this by setting up irq bypass producer's token when handling VHOST_SET_VRING_CALL and un-registering the producer before calling vhost_vring_ioctl() to prevent a possible use after free as eventfd could have been released in vhost_vring_ioctl(). And such registering and unregistering will only be done if DRIVER_OK is set.	2024-10-21	7.8	CVE-2024-47748
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: Fix Use-After-Free of rsv_qp on HIP08 Currently rsv_qp is freed before ib_unregister_device() is called on HIP08. During the time interval, users can still dereg MR and rsv_qp will be used in this process, leading to a UAF. Move the release of rsv_qp after calling ib_unregister_device() to fix it.	2024-10-21	7.8	CVE-2024-47750
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: PCI: kirin: Fix buffer overflow in kirin_pcie_parse_port() Within kirin_pcie_parse_port(), the pcie->num_slots is compared to pcie->gpio_id_reset size (MAX_PCI_SLOTS) which is correct and would lead to an overflow. Thus, fix condition to pcie->num_slots +	2024-10-21	7.8	CVE-2024-47751

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1 >= MAX_PCI_SLOTS and move pcie->num_slots increment below the if-statement to avoid out-of-bounds array access. Found by Linux Verification Center (linuxtesting.org) with SVACE. [kwilczynski: commit log]			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix potential oob read in nilfs_btree_check_delete() The function nilfs_btree_check_delete(), which checks whether degeneration to direct mapping occurs before deleting a b-tree entry, causes memory access outside the block buffer when retrieving the maximum key if the root node has no entries. This does not usually happen because b-tree mappings with 0 child nodes are never created by mkfs.nilfs2 or nilfs2 itself. However, it can happen if the b-tree root node read from a device is configured that way, so fix this potential issue by adding a check for that case.	2024-10-21	7.1	CVE-2024-47757
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: scsi: elx: libefc: Fix potential use after free in efc_nport_vport_del() The kref_put() function will call nport->release if the refcount drops to zero. The nport->release release function is _efc_nport_free() which frees "nport". But then we dereference "nport" on the next line which is a use after free. Re-order these lines to avoid the use after free.	2024-10-21	7.8	CVE-2024-49852
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Fix double free in OPTEE transport Channels can be shared between protocols, avoid freeing the same channel descriptors twice when unloading the stack.	2024-10-21	7.8	CVE-2024-49853
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: block, bfq: fix uaf for accessing waker_bfqq after splitting After commit 42c306ed7233 ("block, bfq: don't break merge chain in bfq_split_bfqq()"), if the current procress is the last holder of bfqq, the bfqq can be freed after bfq_split_bfqq(). Hence recored the bfqq and then access bfqq->waker_bfqq may trigger UAF. What's more, the waker_bfqq may in the merge chain of bfqq, hence just recored waker_bfqq is still not safe. Fix the problem by adding a helper bfq_waker_bfqq() to check if bfqq->waker_bfqq is in the merge chain, and current procress is the only holder.	2024-10-21	7.8	CVE-2024-49854
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: nbd: fix race between timeout and normal completion If request timetout is handled by nbd_requeue_cmd(), normal completion has to be stopped for avoiding to complete this requeued request, other use-after-free can be triggered. Fix the race by clearing NBD_CMD_INFLIGHT in nbd_requeue_cmd(), meantime make sure that cmd->lock is grabbed for clearing the flag and the requeue.	2024-10-21	7	CVE-2024-49855
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ACPI: sysfs: validate return type of _STR method Only buffer objects are valid return values of _STR. If something else is returned description_show() will access invalid memory.	2024-10-21	7.1	CVE-2024-49860
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix helper writes to read-only maps Lonial found an issue that despite user- and BPF-side frozen BPF map (like in case of .rodata), it was still possible to write into it from a BPF program side through specific helpers having ARG_PTR_TO_{LONG,INT} as arguments. In check_func_arg() when the argument is as mentioned, the meta->raw_mode is never set. Later, check_helper_mem_access(), under the case of PTR_TO_MAP_VALUE as register base type, it assumes BPF_READ for the subsequent call to check_map_access_type() and given the BPF map is read-only it succeeds. The helpers really need to be annotated as ARG_PTR_TO_{LONG,INT} | MEM_UNINIT when results are written into them as opposed to read out of them. The latter indicates that it's okay to pass a pointer to uninitialized memory as the memory is written to anyway. However, ARG_PTR_TO_{LONG,INT} is a special case of ARG_PTR_TO_FIXED_SIZE_MEM just with additional alignment requirement. So it is better to just get rid of the ARG_PTR_TO_{LONG,INT} special cases altogether and reuse the fixed size memory types. For this, add	2024-10-21	7.1	CVE-2024-49861

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	MEM_ALIGNED to additionally ensure alignment given these helpers write directly into the args via *<ptr> = val. The .arg*_size has been initialized reflecting the actual sizeof(*<ptr>). MEM_ALIGNED can only be used in combination with MEM_FIXED_SIZE annotated argument types, since in !MEM_FIXED_SIZE cases the verifier does not know the buffer size a priori and therefore cannot blindly write *<ptr> = val.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: powercap: intel_rapl: Fix off by one in get_rpi() The rp->priv->rpi array is either rpi_msr or rpi_tpmi which have NR_RAPL_PRIMITIVES number of elements. Thus the > needs to be >= to prevent an off by one access.	2024-10-21	7.1	CVE-2024-49862
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/xe/vm: move xa_alloc to prevent UAF Evil user can guess the next id of the vm before the ioctl completes and then call vm destroy ioctl to trigger UAF since create ioctl is still referencing the same vm. Move the xa_alloc all the way to the end to prevent this. v2: - Rebase (cherry picked from commit dcfd3971327f3ee92765154baebbaece833d3ca9)	2024-10-21	7.8	CVE-2024-49865
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: btrfs: send: fix buffer overflow detection when copying path to cache entry Starting with commit c0247d289e73 ("btrfs: send: annotate struct name_cache_entry with __counted_by()") we annotated the variable length array "name" from the name_cache_entry structure with __counted_by() to improve overflow detection. However that alone was not correct, because the length of that array does not match the "name_len" field - it matches that plus 1 to include the NUL string terminator, so that makes a fortified kernel think there's an overflow and report a splat like this: strcpy: detected buffer overflow: 20 byte write of buffer size 19 WARNING: CPU: 3 PID: 3310 at __fortify_report+0x45/0x50 CPU: 3 UID: 0 PID: 3310 Comm: btrfs Not tainted 6.11.0-prnet #1 Hardware name: CompuLab Ltd. sbc-ihsw/Intense-PC2 (IPC2), BIOS IPC2_3.330.7 X64 03/15/2018 RIP: 0010:__fortify_report+0x45/0x50 Code: 48 8b 34 (...) RSP: 0018:ffff97ebc0d6f650 EFLAGS: 00010246 RAX: 7749924ef60fa600 RBX: ffff8bf5446a521a RCX: 0000000000000027 RDX: 00000000ffffdfff RSI: ffff97ebc0d6f548 RDI: ffff8bf84e7a1cc8 RBP: ffff8bf548574080 R08: ffffffffa8c40e10 R09: 0000000000005ffd R10: 0000000000000004 R11: ffffffffa8c70e10 R12: ffff8bf551eef400 R13: 0000000000000000 R14: 0000000000000013 R15: 00000000000003a8 FS: 00007fae144de8c0(0000) GS:ffff8bf84e780000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fae14691690 CR3: 00000001027a2003 CR4: 00000000001706f0 Call Trace: <TASK> ? __warn+0x12a/0x1d0 ? __fortify_report+0x45/0x50 ? report_bug+0x154/0x1c0 ? handle_bug+0x42/0x70 ? exc_invalid_op+0x1a/0x50 ? asm_exc_invalid_op+0x1a/0x20 ? __fortify_report+0x45/0x50 __fortify_panic+0x9/0x10 __get_cur_name_and_parent+0x3bc/0x3c0 get_cur_path+0x207/0x3b0 send_extent_data+0x709/0x10d0 ? find_parent_nodes+0x22df/0x25d0 ? mas_nomem+0x13/0x90 ? mtree_insert_range+0xa5/0x110 ? btrfs_lru_cache_store+0x5f/0x1e0 ? iterate_extent_inodes+0x52d/0x5a0 process_extent+0xa96/0x11a0 ? __pfx_lookup_backref_cache+0x10/0x10 ? __pfx_store_backref_cache+0x10/0x10 ? __pfx_iterate_backrefs+0x10/0x10 ? __pfx_check_extent_item+0x10/0x10 changed_cb+0x6fa/0x930 ? tree_advance+0x362/0x390 ? memcmp_extent_buffer+0xd7/0x160 send_subvol+0xf0a/0x1520 btrfs_ioctl_send+0x106b/0x11d0 ? __pfx___clone_root_cmp_sort+0x10/0x10 _btrfs_ioctl_send+0x1ac/0x240 btrfs_ioctl+0x75b/0x850 __se_sys_ioctl+0xca/0x150 do_syscall_64+0x85/0x160 ? __count_memcg_events+0x69/0x100 ? handle_mm_fault+0x1327/0x15c0 ? __se_sys_rt_sigprocmask+0xf1/0x180 ? syscall_exit_to_user_mode+0x75/0xa0 ? do_syscall_64+0x91/0x160 ? do_user_addr_fault+0x21d/0x630 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7fae145eeb4f Code: 00 48 89 (...) RSP: 002b:00007ffdf1cb09b0 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 0000000000000004 RCX:	2024-10-21	7.8	CVE-2024-49869

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	00007fae145eeb4f RDX: 00007ffdf1cb0ad0 RSI: 0000000040489426 RDI: 0000000000000004 RBP: 00000000000078fe R08: 00007fae144006c0 R09: 00007ffdf1cb0927 R10: 0000000000000008 R11: 0000000000000246 R12: 00007ffdf1cb1ce8 R13: 0000000000000003 R14: 000055c499fab2e0 R15: 0000000000000004 </TASK> Fix this by not storing the NUL string terminator since we don't actually need it for name cache entries, this way "name_len" corresponds to the actual size of the "name" array. This requires marking the "name" array field with __nonstring and using memcpy() instead of strcpy() as recommended by the guidelines at: https://github.com/KSPP/linux/issues/90			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: i3c: master: svc: Fix use after free vulnerability in svc_i3c_master Driver Due to Race Condition In the svc_i3c_master_probe function, &master->hj_work is bound with svc_i3c_master_hj_work, &master->ibi_work is bound with svc_i3c_master_ibi_work. And svc_i3c_master_ibi_work can start the hj_work, svc_i3c_master_irq_handler can start the ibi_work. If we remove the module which will call svc_i3c_master_remove to make cleanup, it will free master->base through i3c_master_unregister while the work mentioned above will be used. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | svc_i3c_master_hj_work svc_i3c_master_remove | i3c_master_unregister(&master->base)| device_unregister(&master->dev) | device_release | //free master->base | | i3c_master_do_daa(&master->base) | //use master->base Fix it by ensuring that the work is canceled before proceeding with the cleanup in svc_i3c_master_remove.	2024-10-21	7	CVE-2024-49874
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/xe: fix UAF around queue destruction We currently do stuff like queuing the final destruction step on a random system wq, which will outlive the driver instance. With bad timing we can teardown the driver with one or more work workqueue still being alive leading to various UAF splats. Add a fini step to ensure user queues are properly torn down. At this point GuC should already be nuked so queue itself should no longer be referenced from hw pov. v2 (Matt B) - Looks much safer to use a waitqueue and then just wait for the xa_array to become empty before triggering the drain. (cherry picked from commit 861108666cc0e999cffeab6aff17b662e68774e3)	2024-10-21	7.8	CVE-2024-49876
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ext4: fix off by one issue in alloc_flex_gd() Wesley reported an issue: == EXT4-fs (dm-5): resizing filesystem from 7168 to 786432 blocks ----------[cut here]---------- kernel BUG at fs/ext4/resize.c:324! CPU: 9 UID: 0 PID: 3576 Comm: resize2fs Not tainted 6.11.0+ #27 RIP: 0010:ext4_resize_fs+0x1212/0x12d0 Call Trace: __ext4_ioctl+0x4e0/0x1800 ext4_ioctl+0x12/0x20 __x64_sys_ioctl+0x99/0xd0 x64_sys_call+0x1206/0x20d0 do_syscall_64+0x72/0x110 entry_SYSCALL_64_after_hwframe+0x76/0x7e == While reviewing the patch, Honza found that when adjusting resize_bg in alloc_flex_gd(), it was possible for flex_gd->resize_bg to be bigger than flexbg_size. The reproduction of the problem requires the following: o_group = flexbg_size * 2 * n; o_size = (o_group + 1) * group_size; n_group: [o_group + flexbg_size, o_group + flexbg_size * 2) o_size = (n_group + 1) * group_size; Take n=0,flexbg_size=16 as an example: last:15 |o----------|----------n-| o_group:0 resize to n_group:30 The corresponding reproducer is: img=test.img rm -f $img truncate -s 600M $img mkfs.ext4 -F $img -b 1024 -G 16 8M dev=`losetup -f --show $img` mkdir -p /tmp/test mount $dev /tmp/test resize2fs $dev 248M Delete the problematic plus 1 to fix the issue, and add a WARN_ON_ONCE() to prevent the issue from happening again. [Note: another reproucer which this commit fixes is: img=test.img rm -f $img truncate -s 25MiB $img mkfs.ext4 -b 4096 -E nodiscard,lazy_itable_init=0,lazy_journal_init=0 $img truncate -s 3GiB $img	2024-10-21	7.8	CVE-2024-49880

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	dev=`losetup -f --show $img` mkdir -p /tmp/test mount $dev /tmp/test resize2fs $dev 3G umount $dev losetup -d $dev -- TYT]			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ext4: aovid use-after-free in ext4_ext_insert_extent() As Ojaswin mentioned in Link, in ext4_ext_insert_extent(), if the path is reallocated in ext4_ext_create_new_leaf(), we'll use the stale path and cause UAF. Below is a sample trace with dummy values: ext4_ext_insert_extent path = *ppath = 2000 ext4_ext_create_new_leaf(ppath) ext4_find_extent(ppath) path = *ppath = 2000 if (depth > path[0].p_maxdepth) kfree(path = 2000); *ppath = path = NULL; path = kcalloc() = 3000 *ppath = 3000; return path; /* here path is still 2000, UAF! */ eh = path[depth].p_hdr == BUG: KASAN: slab-use-after-free in ext4_ext_insert_extent+0x26d4/0x3330 Read of size 8 at addr ffff8881027bf7d0 by task kworker/u36:1/179 CPU: 3 UID: 0 PID: 179 Comm: kworker/u6:1 Not tainted 6.11.0-rc2-dirty #866 Call Trace: <TASK> ext4_ext_insert_extent+0x26d4/0x3330 ext4_ext_map_blocks+0xe22/0x2d40 ext4_map_blocks+0x71e/0x1700 ext4_do_writepages+0x1290/0x2800 [...] Allocated by task 179: ext4_find_extent+0x81c/0x1f70 ext4_ext_map_blocks+0x146/0x2d40 ext4_map_blocks+0x71e/0x1700 ext4_do_writepages+0x1290/0x2800 ext4_writepages+0x26d/0x4e0 do_writepages+0x175/0x700 [...] Freed by task 179: kfree+0xcb/0x240 ext4_find_extent+0x7c0/0x1f70 ext4_ext_insert_extent+0xa26/0x3330 ext4_ext_map_blocks+0xe22/0x2d40 ext4_map_blocks+0x71e/0x1700 ext4_do_writepages+0x1290/0x2800 ext4_writepages+0x26d/0x4e0 do_writepages+0x175/0x700 [...] == So use *ppath to update the path to avoid the above problem.	2024-10-21	7.8	CVE-2024-49883
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ext4: fix slab-use-after-free in ext4_split_extent_at() We hit the following use-after-free: == BUG: KASAN: slab-use-after-free in ext4_split_extent_at+0xba8/0xcc0 Read of size 2 at addr ffff88810548ed08 by task kworker/u20:0/40 CPU: 0 PID: 40 Comm: kworker/u20:0 Not tainted 6.9.0-dirty #724 Call Trace: <TASK> kasan_report+0x93/0xc0 ext4_split_extent_at+0xba8/0xcc0 ext4_split_extent.isra.0+0x18f/0x500 ext4_split_convert_extents+0x275/0x750 ext4_ext_handle_unwritten_extents+0x73e/0x1580 ext4_ext_map_blocks+0xe20/0x2dc0 ext4_map_blocks+0x724/0x1700 ext4_do_writepages+0x12d6/0x2a70 [...] Allocated by task 40: __kmalloc_noprof+0x1ac/0x480 ext4_find_extent+0xf3b/0x1e70 ext4_ext_map_blocks+0x188/0x2dc0 ext4_map_blocks+0x724/0x1700 ext4_do_writepages+0x12d6/0x2a70 [...] Freed by task 40: kfree+0xf1/0x2b0 ext4_find_extent+0xa71/0x1e70 ext4_ext_insert_extent+0xa22/0x3260 ext4_split_extent_at+0x3ef/0xcc0 ext4_split_extent.isra.0+0x18f/0x500 ext4_split_convert_extents+0x275/0x750 ext4_ext_handle_unwritten_extents+0x73e/0x1580 ext4_ext_map_blocks+0xe20/0x2dc0 ext4_map_blocks+0x724/0x1700 ext4_do_writepages+0x12d6/0x2a70 [...] == The flow of issue triggering is as follows: ext4_split_extent_at path = *ppath ext4_ext_insert_extent(ppath) ext4_ext_create_new_leaf(ppath) ext4_find_extent(orig_path) path = *orig_path read_extent_tree_block // return -ENOMEM or -EIO ext4_free_ext_path(path) kfree(path) *orig_path = NULL a. If err is -ENOMEM: ext4_ext_dirty(path + path->p_depth) // path use-after-free !!! b. If err is -EIO and we have EXT_DEBUG defined: ext4_ext_show_leaf(path) eh = path[depth].p_hdr // path also use-after-free !!! So when trying to zeroout or fix the extent length, call ext4_find_extent() to update the path. In addition we use *ppath directly as an ext4_ext_show_leaf() input to avoid possible use-after-free when EXT_DEBUG is defined, and to avoid unnecessary path updates.	2024-10-21	7.8	CVE-2024-49884

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ext4: avoid use-after-free in ext4_ext_show_leaf() In ext4_find_extent(), path may be freed by error or be reallocated, so using a previously saved *ppath may have been freed and thus may trigger use-after-free, as follows: ext4_split_extent path = *ppath; ext4_split_extent_at(ppath) path = ext4_find_extent(ppath) ext4_split_extent_at(ppath) // ext4_find_extent fails to free path // but zeroout succeeds ext4_ext_show_leaf(inode, path) eh = path[depth].p_hdr // path use-after-free !!! Similar to ext4_split_extent_at(), we use *ppath directly as an input to ext4_ext_show_leaf(). Fix a spelling error by the way. Same problem in ext4_ext_handle_unwritten_extents(). Since 'path' is only used in ext4_ext_show_leaf(), remove 'path' and use *ppath directly. This issue is triggered only when EXT_DEBUG is defined and therefore does not affect functionality.	2024-10-21	7.8	CVE-2024-49889
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix index out of bounds in degamma hardware format translation Fixes index out of bounds issue in `cm_helper_translate_curve_to_degamma_hw_format` function. The issue could occur when the index 'i' exceeds the number of transfer function points (TRANSFER_FUNC_POINTS). The fix adds a check to ensure 'i' is within bounds before accessing the transfer function points. If 'i' is out of bounds the function returns false to indicate an error. Reported by smatch: drivers/gpu/drm/amd/amdgpu/../display/dc/dcn10/dcn10_cm_common.c:594 cm_helper_translate_curve_to_degamma_hw_format() error: buffer overflow 'output_tf->tf_pts.red' 1025 <= s32max drivers/gpu/drm/amd/amdgpu/../display/dc/dcn10/dcn10_cm_common.c:595 cm_helper_translate_curve_to_degamma_hw_format() error: buffer overflow 'output_tf->tf_pts.green' 1025 <= s32max drivers/gpu/drm/amd/amdgpu/../display/dc/dcn10/dcn10_cm_common.c:596 cm_helper_translate_curve_to_degamma_hw_format() error: buffer overflow 'output_tf->tf_pts.blue' 1025 <= s32max	2024-10-21	7.8	CVE-2024-49894
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix index out of bounds in DCN30 degamma hardware format translation This commit addresses a potential index out of bounds issue in the `cm3_helper_translate_curve_to_degamma_hw_format` function in the DCN30 color management module. The issue could occur when the index 'i' exceeds the number of transfer function points (TRANSFER_FUNC_POINTS). The fix adds a check to ensure 'i' is within bounds before accessing the transfer function points. If 'i' is out of bounds, the function returns false to indicate an error. Reported by smatch: drivers/gpu/drm/amd/amdgpu/../display/dc/dcn30/dcn30_cm_common.c:338 cm3_helper_translate_curve_to_degamma_hw_format() error: buffer overflow 'output_tf->tf_pts.red' 1025 <= s32max drivers/gpu/drm/amd/amdgpu/../display/dc/dcn30/dcn30_cm_common.c:339 cm3_helper_translate_curve_to_degamma_hw_format() error: buffer overflow 'output_tf->tf_pts.green' 1025 <= s32max drivers/gpu/drm/amd/amdgpu/../display/dc/dcn30/dcn30_cm_common.c:340 cm3_helper_translate_curve_to_degamma_hw_format() error: buffer overflow 'output_tf->tf_pts.blue' 1025 <= s32max	2024-10-21	7.8	CVE-2024-49895
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix uninit-value access of new_ea in ea_buffer syzbot reports that lzo1x_1_do_compress is using uninit-value: === BUG: KMSAN: uninit-value in lzo1x_1_do_compress+0x19f9/0x2510 lib/lzo/lzo1x_compress.c:178 ... Uninit was stored to memory at: ea_put fs/jfs/xattr.c:639 [inline] ... Local variable ea_buf created at: __jfs_setxattr+0x5d/0x1ae0 fs/jfs/xattr.c:662 __jfs_xattr_set+0xe6/0x1f0 fs/jfs/xattr.c:934 ===	2024-10-21	7.1	CVE-2024-49900

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The reason is ea_buf->new_ea is not initialized properly. Fix this by using memset to empty its content at the beginning in ea_get().			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix uaf in dbFreeBits [syzbot reported] == BUG: KASAN: slab-use-after-free in __mutex_lock_common kernel/locking/mutex.c:587 [inline] BUG: KASAN: slab-use-after-free in __mutex_lock+0xfe/0xd70 kernel/locking/mutex.c:752 Read of size 8 at addr ffff8880229254b0 by task syz-executor357/5216 CPU: 0 UID: 0 PID: 5216 Comm: syz-executor357 Not tainted 6.11.0-rc3-syzkaller-00156-gd7a5aa4b3c00 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 __mutex_lock_common kernel/locking/mutex.c:587 [inline] __mutex_lock+0xfe/0xd70 kernel/locking/mutex.c:752 dbFreeBits+0x7ea/0xd90 fs/jfs/jfs_dmap.c:2390 dbFreeDmap fs/jfs/jfs_dmap.c:2089 [inline] dbFree+0x35b/0x680 fs/jfs/jfs_dmap.c:409 dbDiscardAG+0x8a9/0xa20 fs/jfs/jfs_dmap.c:1650 jfs_ioc_trim+0x433/0x670 fs/jfs/jfs_discard.c:100 jfs_ioctl+0x2d0/0x3e0 fs/jfs/ioctl.c:131 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl+0xfc/0x170 fs/ioctl.c:893 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 Freed by task 5218: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579 poison_slab_object+0xe0/0x150 mm/kasan/common.c:240 __kasan_slab_free+0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2252 [inline] slab_free mm/slub.c:4473 [inline] kfree+0x149/0x360 mm/slub.c:4594 dbUnmount+0x11d/0x190 fs/jfs/jfs_dmap.c:278 jfs_mount_rw+0x4ac/0x6a0 fs/jfs/jfs_mount.c:247 jfs_remount+0x3d1/0x6b0 fs/jfs/super.c:454 reconfigure_super+0x445/0x880 fs/super.c:1083 vfs_cmd_reconfigure fs/fsopen.c:263 [inline] vfs_fsconfig_locked fs/fsopen.c:292 [inline] __do_sys_fsconfig fs/fsopen.c:473 [inline] __se_sys_fsconfig+0xb6e/0xf80 fs/fsopen.c:345 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f [Analysis] There are two paths (dbUnmount and jfs_ioc_trim) that generate race condition when accessing bmap, which leads to the occurrence of uaf. Use the lock s_umount to synchronize them, in order to avoid uaf caused by race condition.	2024-10-21	7	CVE-2024-49903
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: fbdev: pxafb: Fix possible use after free in pxafb_task() In the pxafb_probe function, it calls the pxafb_init_fbinfo function, after which &fbi->task is associated with pxafb_task. Moreover, within this pxafb_init_fbinfo function, the pxafb_blank function within the &pxafb_ops struct is capable of scheduling work. If we remove the module which will call pxafb_remove to make cleanup, it will call unregister_framebuffer function which can call do_unregister_framebuffer to free fbi->fb through put_fb_info(fb_info), while the work mentioned above will be used. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | pxafb_task pxafb_remove | unregister_framebuffer(info) | do_unregister_framebuffer(fb_info) | put_fb_info(fb_info) | // free fbi->fb | set_ctrlr_state(fbi, state) | __pxafb_lcd_power(fbi, 0) | fbi->lcd_power(on, &fbi->fb.var) | //use fbi->fb Fix it by ensuring that the work is canceled before proceeding with the cleanup in pxafb_remove. Note that only root user can remove the driver at runtime.	2024-10-21	7.8	CVE-2024-49924

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: avoid reading out of bounds when loading TX power FW elements Because the loop-expression will do one more time before getting false from cond-expression, the original code copied one more entry size beyond valid region. Fix it by moving the entry copy to loop-body.	2024-10-21	7.1	CVE-2024-49928
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: fix array out-of-bound access in SoC stats Currently, the ath11k_soc_dp_stats::hal_reo_error array is defined with a maximum size of DP_REO_DST_RING_MAX. However, the ath11k_dp_process_rx() function access ath11k_soc_dp_stats::hal_reo_error using the REO destination SRNG ring ID, which is incorrect. SRNG ring ID differ from normal ring ID, and this usage leads to out-of-bounds array access. To fix this issue, modify ath11k_dp_process_rx() to use the normal ring ID directly instead of the SRNG ring ID to avoid out-of-bounds array access. Tested-on: QCN9074 hw1.0 PCI WLAN.HK.2.7.0.1-01744-QCAHKSWPL_SILICONZ-1	2024-10-21	7.8	CVE-2024-49930
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix array out-of-bound access in SoC stats Currently, the ath12k_soc_dp_stats::hal_reo_error array is defined with a maximum size of DP_REO_DST_RING_MAX. However, the ath12k_dp_rx_process() function access ath12k_soc_dp_stats::hal_reo_error using the REO destination SRNG ring ID, which is incorrect. SRNG ring ID differ from normal ring ID, and this usage leads to out-of-bounds array access. To fix this issue, modify ath12k_dp_rx_process() to use the normal ring ID directly instead of the SRNG ring ID to avoid out-of-bounds array access. Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.0.1-00029-QCAHKSWPL_SILICONZ-1	2024-10-21	7.8	CVE-2024-49931
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net/xen-netback: prevent UAF in xenvif_flush_hash() During the list_for_each_entry_rcu iteration call of xenvif_flush_hash, kfree_rcu does not exist inside the rcu read critical section, so if kfree_rcu is called when the rcu grace period ends during the iteration, UAF occurs when accessing head->next after the entry becomes free. Therefore, to solve this, you need to change it to list_for_each_entry_safe.	2024-10-21	7.8	CVE-2024-49936
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix index out of bounds in DCN30 color transformation This commit addresses a potential index out of bounds issue in the `cm3_helper_translate_curve_to_hw_format` function in the DCN30 color management module. The issue could occur when the index 'i' exceeds the number of transfer function points (TRANSFER_FUNC_POINTS). The fix adds a check to ensure 'i' is within bounds before accessing the transfer function points. If 'i' is out of bounds, the function returns false to indicate an error. drivers/gpu/drm/amd/amdgpu/../display/dc/dcn30/dcn30_cm_common.c:180 cm3_helper_translate_curve_to_hw_format() error: buffer overflow 'output_tf->tf_pts.red' 1025 <= s32max drivers/gpu/drm/amd/amdgpu/../display/dc/dcn30/dcn30_cm_common.c:181 cm3_helper_translate_curve_to_hw_format() error: buffer overflow 'output_tf->tf_pts.green' 1025 <= s32max drivers/gpu/drm/amd/amdgpu/../display/dc/dcn30/dcn30_cm_common.c:182 cm3_helper_translate_curve_to_hw_format() error: buffer overflow 'output_tf->tf_pts.blue' 1025 <= s32max	2024-10-21	7.8	CVE-2024-49969
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: media: venus: fix use after free bug in venus_remove due to race condition in venus_probe, core->work is bound with venus_sys_error_handler, which is used to handle error. The code use core->sys_err_done to make sync work. The core->work is started in venus_event_notify. If we call venus_remove, there might be an unfished work. The possible sequence is as follows: CPU0 CPU1 |venus_sys_error_handler venus_remove | hfi_destroy | venus_hfi_destroy | kfree(hdev); | |hfi_reinit	2024-10-21	7	CVE-2024-49981

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	|venus_hfi_queues_reinit |//use hdev Fix it by canceling the work in venus_remove.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem in more places For fixing CVE-2023-6270, f98364e92662 ("aoe: fix the potential use-after-free problem in aoecmd_cfg_pkts") makes tx() calling dev_put() instead of doing in aoecmd_cfg_pkts(). It avoids that the tx() runs into use-after-free. Then Nicolai Stange found more places in aoe have potential use-after-free problem with tx(). e.g. revalidate(), aoecmd_ata_rw(), resend(), probe() and aoecmd_cfg_rsp(). Those functions also use aoenet_xmit() to push packet to tx queue. So they should also use dev_hold() to increase the refcnt of skb->dev. On the other hand, moving dev_put() to tx() causes that the refcnt of skb->dev be reduced to a negative value, because corresponding dev_hold() are not called in revalidate(), aoecmd_ata_rw(), resend(), probe(), and aoecmd_cfg_rsp(). This patch fixed this issue.	2024-10-21	7.8	CVE-2024-49982
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: platform/x86: x86-android-tablets: Fix use after free on platform_device_register() errors x86_android_tablet_remove() frees the pdevs[] array, so it should not be used after calling x86_android_tablet_remove(). When platform_device_register() fails, store the pdevs[x] PTR_ERR() value into the local ret variable before calling x86_android_tablet_remove() to avoid using pdevs[] after it has been freed.	2024-10-21	7.8	CVE-2024-49986
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: fix double free issue during amdgpu module unload Flexible endpoints use DIGs from available inflexible endpoints, so only the encoders of inflexible links need to be freed. Otherwise, a double free issue may occur when unloading the amdgpu module. [279.190523] RIP: 0010:__slab_free+0x152/0x2f0 [279.190577] Call Trace: [279.190580] <TASK> [279.190582] ? show_regs+0x69/0x80 [279.190590] ? die+0x3b/0x90 [279.190595] ? do_trap+0xc8/0xe0 [279.190601] ? do_error_trap+0x73/0xa0 [279.190605] ? __slab_free+0x152/0x2f0 [279.190609] ? exc_invalid_op+0x56/0x70 [279.190616] ? __slab_free+0x152/0x2f0 [279.190642] ? asm_exc_invalid_op+0x1f/0x30 [279.190648] ? dcn10_link_encoder_destroy+0x19/0x30 [amdgpu] [279.191096] ? __slab_free+0x152/0x2f0 [279.191102] ? dcn10_link_encoder_destroy+0x19/0x30 [amdgpu] [279.191469] kfree+0x260/0x2b0 [279.191474] dcn10_link_encoder_destroy+0x19/0x30 [amdgpu] [279.191821] link_destroy+0xd7/0x130 [amdgpu] [279.192248] dc_destruct+0x90/0x270 [amdgpu] [279.192666] dc_destroy+0x19/0x40 [amdgpu] [279.193020] amdgpu_dm_fini+0x16e/0x200 [amdgpu] [279.193432] dm_hw_fini+0x26/0x40 [amdgpu] [279.193795] amdgpu_device_fini_hw+0x24c/0x400 [amdgpu] [279.194108] amdgpu_driver_unload_kms+0x4f/0x70 [amdgpu] [279.194436] amdgpu_pci_remove+0x40/0x80 [amdgpu] [279.194632] pci_device_remove+0x3a/0xa0 [279.194638] device_remove+0x40/0x70 [279.194642] device_release_driver_internal+0x1ad/0x210 [279.194647] driver_detach+0x4e/0xa0 [279.194650] bus_remove_driver+0x6f/0xf0 [279.194653] driver_unregister+0x33/0x60 [279.194657] pci_unregister_driver+0x44/0x90 [279.194662] amdgpu_exit+0x19/0x1f0 [amdgpu] [279.194939] __do_sys_delete_module.isra.0+0x198/0x2f0 [279.194946] __x64_sys_delete_module+0x16/0x20 [279.194950] do_syscall_64+0x58/0x120 [279.194954] entry_SYSCALL_64_after_hwframe+0x6e/0x76 [279.194980] </TASK>	2024-10-21	7.8	CVE-2024-49989
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/stm: Avoid use-after-free issues with crtc and plane ltdc_load() calls functions drm_crtc_init_with_planes(), drm_universal_plane_init() and drm_encoder_init(). These functions should not be called with parameters allocated with devm_kzalloc() to avoid use-after-free issues [1]. Use allocations managed by the	2024-10-21	7.8	CVE-2024-49992

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	DRM framework. Found by Linux Verification Center (linuxtesting.org). [1] https://lore.kernel.org/lkml/u366i76e3qhh3ra5oxrtngjtm2u5lterkekcz6y2jkndhuxzli@diujon4h7qwb/			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: cifs: Fix buffer overflow when parsing NFS reparse points ReparseDataLength is sum of the InodeType size and DataBuffer size. So to get DataBuffer size it is needed to subtract InodeType's size from ReparseDataLength. Function cifs_strndup_from_utf16() is currentlly accessing buf->DataBuffer at position after the end of the buffer because it does not subtract InodeType size from the length. Fix this problem and correctly subtract variable len. Member InodeType is present only when reparse buffer is large enough. Check for ReparseDataLength before accessing InodeType to prevent another invalid memory access. Major and minor rdev values are present also only when reparse buffer is large enough. Check for reparse buffer size before calling reparse_mkdev().	2024-10-21	7.8	CVE-2024-49996
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_conn: Fix UAF in hci_enhanced_setup_sync This checks if the ACL connection remains valid as it could be destroyed while hci_enhanced_setup_sync is pending on cmd_sync leading to the following trace: BUG: KASAN: slab-use-after-free in hci_enhanced_setup_sync+0x91b/0xa60 Read of size 1 at addr ffff888002328ffd by task kworker/u5:2/37 CPU: 0 UID: 0 PID: 37 Comm: kworker/u5:2 Not tainted 6.11.0-rc6-01300-g810be445d8d6 #7099 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 Workqueue: hci0 hci_cmd_sync_work Call Trace: <TASK> dump_stack_lvl+0x5d/0x80 ? hci_enhanced_setup_sync+0x91b/0xa60 print_report+0x152/0x4c0 ? hci_enhanced_setup_sync+0x91b/0xa60 ? __virt_addr_valid+0x1fa/0x420 ? hci_enhanced_setup_sync+0x91b/0xa60 kasan_report+0xda/0x1b0 ? hci_enhanced_setup_sync+0x91b/0xa60 hci_enhanced_setup_sync+0x91b/0xa60 ? __pfx_hci_enhanced_setup_sync+0x10/0x10 ? __pfx___mutex_lock+0x10/0x10 hci_cmd_sync_work+0x1c2/0x330 process_one_work+0x7d9/0x1360 ? __pfx_lock_acquire+0x10/0x10 ? __pfx_process_one_work+0x10/0x10 ? assign_work+0x167/0x240 worker_thread+0x5b7/0xf60 ? __kthread_parkme+0xac/0x1c0 ? __pfx_worker_thread+0x10/0x10 ? __pfx_worker_thread+0x10/0x10 kthread+0x293/0x360 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2f/0x70 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> Allocated by task 34: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x8f/0xa0 __hci_conn_add+0x187/0x17d0 hci_connect_sco+0x2e1/0xb90 sco_sock_connect+0x2a2/0xb80 __sys_connect+0x227/0x2a0 __x64_sys_connect+0x6d/0xb0 do_syscall_64+0x71/0x140 entry_SYSCALL_64_after_hwframe+0x76/0x7e Freed by task 37: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x60 __kasan_slab_free+0x101/0x160 kfree+0xd0/0x250 device_release+0x9a/0x210 kobject_put+0x151/0x280 hci_conn_del+0x448/0xbf0 hci_abort_conn_sync+0x46f/0x980 hci_cmd_sync_work+0x1c2/0x330 process_one_work+0x7d9/0x1360 worker_thread+0x5b7/0xf60 kthread+0x293/0x360 ret_from_fork+0x2f/0x70 ret_from_fork_asm+0x1a/0x30	2024-10-21	7.8	CVE-2024-50029
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/xe/ct: prevent UAF in send_recv() Ensure we serialize with completion side to prevent UAF with fence going out of scope on the stack, since we have no clue if it will fire after the timeout before we can erase from the xa. Also we have some dependent loads and stores for which we need the correct ordering, and we lack the needed barriers. Fix this by grabbing the ct->lock after the wait, which is also held by the completion side. v2 (Badal): - Also print done after acquiring the lock and seeing timeout. (cherry picked from commit 52789ce35c55ccd30c4b67b9cc5b2af55e0122ea)	2024-10-21	7.8	CVE-2024-50030

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: slip: make slhc_remember() more robust against malicious packets syzbot found that slhc_remember() was missing checks against malicious packets [1]. slhc_remember() only checked the size of the packet was at least 20, which is not good enough. We need to make sure the packet includes the IPv4 and TCP header that are supposed to be carried. Add iph and th pointers to make the code more readable. [1] BUG: KMSAN: uninit-value in slhc_remember+0x2e8/0x7b0 drivers/net/slip/slhc.c:666 slhc_remember+0x2e8/0x7b0 drivers/net/slip/slhc.c:666 ppp_receive_nonmp_frame+0xe45/0x35e0 drivers/net/ppp/ppp_generic.c:2455 ppp_receive_frame drivers/net/ppp/ppp_generic.c:2372 [inline] ppp_do_recv+0x65f/0x40d0 drivers/net/ppp/ppp_generic.c:2212 ppp_input+0x7dc/0xe60 drivers/net/ppp/ppp_generic.c:2327 pppoe_rcv_core+0x1d3/0x720 drivers/net/ppp/pppoe.c:379 sk_backlog_rcv+0x13b/0x420 include/net/sock.h:1113 __release_sock+0x1da/0x330 net/core/sock.c:3072 release_sock+0x6b/0x250 net/core/sock.c:3626 pppoe_sendmsg+0x2b8/0xb90 drivers/net/ppp/pppoe.c:903 sock_sendmsg_nosec net/socket.c:729 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:744 ____sys_sendmsg+0x903/0xb60 net/socket.c:2602 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2656 __sys_sendmmsg+0x3c1/0x960 net/socket.c:2742 __do_sys_sendmmsg net/socket.c:2771 [inline] __se_sys_sendmmsg net/socket.c:2768 [inline] __x64_sys_sendmmsg+0xbc/0x120 net/socket.c:2768 x64_sys_call+0xb6e/0x3ba0 arch/x86/include/generated/asm/syscalls_64.h:308 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:4091 [inline] slab_alloc_node mm/slub.c:4134 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4186 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:587 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:678 alloc_skb include/linux/skbuff.h:1322 [inline] sock_wmalloc+0xfe/0x1a0 net/core/sock.c:2732 pppoe_sendmsg+0x3a7/0xb90 drivers/net/ppp/pppoe.c:867 sock_sendmsg_nosec net/socket.c:729 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:744 ____sys_sendmsg+0x903/0xb60 net/socket.c:2602 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2656 __sys_sendmmsg+0x3c1/0x960 net/socket.c:2742 __do_sys_sendmmsg net/socket.c:2771 [inline] __se_sys_sendmmsg net/socket.c:2768 [inline] __x64_sys_sendmmsg+0xbc/0x120 net/socket.c:2768 x64_sys_call+0xb6e/0x3ba0 arch/x86/include/generated/asm/syscalls_64.h:308 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 5460 Comm: syz.2.33 Not tainted 6.12.0-rc2-syzkaller-00006-g87d6aab2389e #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024	2024-10-21	7.1	CVE-2024-50033
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ppp: fix ppp_async_encode() illegal access syzbot reported an issue in ppp_async_encode() [1] In this case, pppoe_sendmsg() is called with a zero size. Then ppp_async_encode() is called with an empty skb. BUG: KMSAN: uninit-value in ppp_async_encode drivers/net/ppp/ppp_async.c:545 [inline] BUG: KMSAN: uninit-value in ppp_async_push+0xb4f/0x2660 drivers/net/ppp/ppp_async.c:675 ppp_async_encode drivers/net/ppp/ppp_async.c:545 [inline] ppp_async_push+0xb4f/0x2660 drivers/net/ppp/ppp_async.c:675 ppp_async_send+0x130/0x1b0 drivers/net/ppp/ppp_async.c:634 ppp_channel_bridge_input drivers/net/ppp/ppp_generic.c:2280 [inline] ppp_input+0x1f1/0xe60 drivers/net/ppp/ppp_generic.c:2304 pppoe_rcv_core+0x1d3/0x720 drivers/net/ppp/pppoe.c:379 sk_backlog_rcv+0x13b/0x420 include/net/sock.h:1113 __release_sock+0x1da/0x330 net/core/sock.c:3072 release_sock+0x6b/0x250 net/core/sock.c:3626 pppoe_sendmsg+0x2b8/0xb90 drivers/net/ppp/pppoe.c:903 sock_sendmsg_nosec net/socket.c:729 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:744 ____sys_sendmsg+0x903/0xb60	2024-10-21	7.1	CVE-2024-50035

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	net/socket.c:2602 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2656 __sys_sendmmsg+0x3c1/0x960 net/socket.c:2742 __do_sys_sendmmsg net/socket.c:2771 [inline] __se_sys_sendmmsg net/socket.c:2768 [inline] __x64_sys_sendmmsg+0xbc/0x120 net/socket.c:2768 x64_sys_call+0xb6e/0x3ba0 arch/x86/include/generated/asm/syscalls_64.h:308 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:4092 [inline] slab_alloc_node mm/slub.c:4135 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4187 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:587 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:678 alloc_skb include/linux/skbuff.h:1322 [inline] sock_wmalloc+0xfe/0x1a0 net/core/sock.c:2732 pppoe_sendmsg+0x3a7/0xb90 drivers/net/ppp/pppoe.c:867 sock_sendmsg_nosec net/socket.c:729 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:744 ____sys_sendmsg+0x903/0xb60 net/socket.c:2602 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2656 __sys_sendmmsg+0x3c1/0x960 net/socket.c:2742 __do_sys_sendmmsg net/socket.c:2771 [inline] __se_sys_sendmmsg net/socket.c:2768 [inline] __x64_sys_sendmmsg+0xbc/0x120 net/socket.c:2768 x64_sys_call+0xb6e/0x3ba0 arch/x86/include/generated/asm/syscalls_64.h:308 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 1 UID: 0 PID: 5411 Comm: syz.1.14 Not tainted 6.12.0-rc1-syzkaller-00165-g360c1f1f24c6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: do not delay dst_entries_add() in dst_release() dst_entries_add() uses per-cpu data that might be freed at netns dismantle from ip6_route_net_exit() calling dst_entries_destroy() Before ip6_route_net_exit() can be called, we release all the dsts associated with this netns, via calls to dst_release(), which waits an rcu grace period before calling dst_destroy() dst_entries_add() use in dst_destroy() is racy, because dst_entries_destroy() could have been called already. Decrementing the number of dsts must happen sooner. Notes: 1) in CONFIG_XFRM case, dst_destroy() can call dst_release_immediate(child), this might also cause UAF if the child does not have DST_NOCOUNT set. IPSEC maintainers might take a look and see how to address this. 2) There is also discussion about removing this count of dst, which might happen in future kernels.	2024-10-21	7	CVE-2024-50036
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix possible badness in FREE_STATEID When multiple FREE_STATEIDs are sent for the same delegation stateid, it can lead to a possible either use-after-free or counter refcount underflow errors. In nfsd4_free_stateid() under the client lock we find a delegation stateid, however the code drops the lock before calling nfs4_put_stid(), that allows another FREE_STATE to find the stateid again. The first one will proceed to then free the stateid which leads to either use-after-free or decrementing already zeroed counter.	2024-10-21	7.8	CVE-2024-50043
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix UAF in async decryption Doing an async decryption (large read) crashes with a slab-use-after-free way down in the crypto API. Reproducer: # mount.cifs -o ...,seal,esize=1 //srv/share /mnt # dd if=/mnt/largefile of=/dev/null ... [194.196391] == [194.196844] BUG: KASAN: slab-use-after-free in gf128mul_4k_lle+0xc1/0x110 [194.197269] Read of size 8 at addr ffff888112bd0448 by task kworker/u77:2/899 [194.197707] [194.197818] CPU: 12 UID: 0 PID: 899 Comm: kworker/u77:2 Not tainted 6.11.0-lku-00028-gfca3ca14a17a-dirty #43 [194.198400] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.16.2-3-gd478f380-prebuilt.qemu.org 04/01/2014 [194.199046] Workqueue: smb3decryptd smb2_decrypt_offload [cifs] [194.200032] Call Trace: [194.200191] <TASK> [	2024-10-21	7.8	CVE-2024-50047

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	194.200327] dump_stack_lvl+0x4e/0x70 [194.200558] ? gf128mul_4k_lle+0xc1/0x110 [194.200809] print_report+0x174/0x505 [194.201040] ? __pfx__raw_spin_lock_irqsave+0x10/0x10 [194.201352] ? srso_return_thunk+0x5/0x5f [194.201604] ? __virt_addr_valid+0xdf/0x1c0 [194.201868] ? gf128mul_4k_lle+0xc1/0x110 [194.202128] kasan_report+0xc8/0x150 [194.202361] ? gf128mul_4k_lle+0xc1/0x110 [194.202616] gf128mul_4k_lle+0xc1/0x110 [194.202863] ghash_update+0x184/0x210 [194.203103] shash_ahash_update+0x184/0x2a0 [194.203377] ? __pfx_shash_ahash_update+0x10/0x10 [194.203651] ? srso_return_thunk+0x5/0x5f [194.203877] ? crypto_gcm_init_common+0x1ba/0x340 [194.204142] gcm_hash_assoc_remain_continue+0x10a/0x140 [194.204434] crypt_message+0xec1/0x10a0 [cifs] [194.206489] ? __pfx_crypt_message+0x10/0x10 [cifs] [194.208507] ? srso_return_thunk+0x5/0x5f [194.209205] ? srso_return_thunk+0x5/0x5f [194.209925] ? srso_return_thunk+0x5/0x5f [194.210443] ? srso_return_thunk+0x5/0x5f [194.211037] decrypt_raw_data+0x15f/0x250 [cifs] [194.212906] ? __pfx_decrypt_raw_data+0x10/0x10 [cifs] [194.214670] ? srso_return_thunk+0x5/0x5f [194.215193] smb2_decrypt_offload+0x12a/0x6c0 [cifs] This is because TFM is being used in parallel. Fix this by allocating a new AEAD TFM for async decryption, but keep the existing one for synchronous READ cases (similar to what is done in smb3_calc_signature()). Also remove the calls to aead_request_set_callback() and crypto_wait_req() since it's always going to be a synchronous operation.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: driver core: bus: Fix double free in driver API bus_register() For bus_register(), any error which happens after kset_register() will cause that @priv are freed twice, fixed by setting @priv with NULL after the first free.	2024-10-21	7.8	CVE-2024-50055
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ntb: ntb_hw_switchtec: Fix use after free vulnerability in switchtec_ntb_remove due to race condition In the switchtec_ntb_add function, it can call switchtec_ntb_init_sndev function, then &sndev->check_link_status_work is bound with check_link_status_work. switchtec_ntb_link_notification may be called to start the work. If we remove the module which will call switchtec_ntb_remove to make cleanup, it will free sndev through kfree(sndev), while the work mentioned above will be used. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | check_link_status_work switchtec_ntb_remove | kfree(sndev); | | if (sndev->link_force_down) | // use sndev Fix it by ensuring that the work is canceled before proceeding with the cleanup in switchtec_ntb_remove.	2024-10-21	7	CVE-2024-50059
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: i3c: master: cdns: Fix use after free vulnerability in cdns_i3c_master Driver Due to Race Condition In the cdns_i3c_master_probe function, &master->hj_work is bound with cdns_i3c_master_hj. And cdns_i3c_master_interrupt can call cnds_i3c_master_demux_ibis function to start the work. If we remove the module which will call cdns_i3c_master_remove to make cleanup, it will free master->base through i3c_master_unregister while the work mentioned above will be used. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | cdns_i3c_master_hj cdns_i3c_master_remove | i3c_master_unregister(&master->base) | device_unregister(&master->dev) | device_release | //free master->base | | i3c_master_do_daa(&master->base) | //use master->base Fix it by ensuring that the work is canceled before proceeding with the cleanup in cdns_i3c_master_remove.	2024-10-21	7	CVE-2024-50061
ManageEngine-- ADAudit Plus	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to SQL Injection in the technician reports feature.	2024-10-24	8.3	CVE-2024-5608

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mapster--Mapster WP Maps	The Mapster WP Maps plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to an insufficient capability check on the mapster_wp_maps_set_option_from_js() function in all versions up to, and including, 1.5.0. This makes it possible for authenticated attackers, with contributor-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	2024-10-25	8.8	CVE-2024-9235
mitel -- micollab	A vulnerability in the Suite Applications Services component of Mitel MiCollab through 9.7.1.110 could allow an authenticated attacker with administrative privileges to conduct a SQL Injection attack due to insufficient validation of user input. A successful exploit could allow an attacker to execute arbitrary database and management operations.	2024-10-21	7.2	CVE-2024-30157
mitel -- micollab	A vulnerability in the web conferencing component of Mitel MiCollab through 9.7.1.110 could allow an authenticated attacker with administrative privileges to conduct a SQL Injection attack due to insufficient validation of user input. A successful exploit could allow an attacker to execute arbitrary database and management operations.	2024-10-21	7.2	CVE-2024-30158
Mitsubishi Electric Corporation--GENESIS64	Incorrect Default Permissions vulnerability in GenBroker32, which is included in the installers for ICONICS GENESIS64 version 10.97.3 and prior, Mitsubishi Electric GENESIS64 version 10.97.3 and prior and Mitsubishi Electric MC Works64 all versions allows a local authenticated attacker to disclose or tamper with confidential information and data contained in the products, or cause a denial of service (DoS) condition on the products, by accessing a folder with incorrect permissions, when GenBroker32 is installed on the same PC as GENESIS64 or MC Works64.	2024-10-22	7.8	CVE-2024-7587
mohammed_kaludi--AMP for WP Accelerated Mobile Pages	The AMP for WP - Accelerated Mobile Pages plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.99.1. This is due to missing or incorrect nonce validation on the 'proxy' function. This makes it possible for unauthenticated attackers to send the logged in user's cookies to their own server via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-10-25	8.8	CVE-2024-9598
n/a--n/a	OvalEdge 5.2.8.0 and earlier is affected by an Account Takeover vulnerability via a POST request to /profile/updateProfile via the userId and email parameters. Authentication is required.	2024-10-25	9.8	CVE-2022-30355
n/a--n/a	OvalEdge 5.2.8.0 and earlier is affected by an Account Takeover vulnerability via a POST request to /profile/updateProfile via the userId and email parameters. Authentication is required.	2024-10-25	9.8	CVE-2022-30357
n/a--n/a	An issue in Casa Systems NTC-221 version 2.0.99.0 and before allows a remote attacker to execute arbitrary code via a crafted payload to the /www/cgi-bin/nas.cgi component.	2024-10-22	9	CVE-2024-26519
n/a--n/a	A vulnerability in NuPoint Messenger (NPM) of Mitel MiCollab through 9.8.0.33 allows an unauthenticated attacker to conduct a command injection attack due to insufficient parameter sanitization.	2024-10-21	9.8	CVE-2024-35285
n/a--n/a	A vulnerability in NuPoint Messenger (NPM) of Mitel MiCollab through 9.8.0.33 allows an unauthenticated attacker to conduct a SQL injection attack due to insufficient sanitization of user input. A successful exploit could allow an attacker to access sensitive information and execute arbitrary database and management operations.	2024-10-21	9.8	CVE-2024-35286
n/a--n/a	A vulnerability in the Desktop Client of Mitel MiCollab through 9.7.1.110, and MiVoice Business Solution Virtual Instance (MiVB SVI) 1.0.0.25, could allow an	2024-10-21	9.8	CVE-2024-35314

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated attacker to conduct a command injection attack due to insufficient parameter sanitization. A successful exploit could allow an attacker to execute arbitrary scripts.			
n/a--n/a	A Buffer Overflow vulnerabilty in the local_app_set_router_token function of Vilo 5 Mesh WiFi System <= 5.16.1.33 allows remote, unauthenticated attackers to execute arbitrary code via sscanf reading the token and timezone JSON fields into a fixed-length buffer.	2024-10-21	9.6	CVE-2024-40083
n/a--n/a	A Buffer Overflow in the Boa webserver of Vilo 5 Mesh WiFi System <= 5.16.1.33 allows remote, unauthenticated attackers to execute arbitrary code via exceptionally long HTTP methods or paths.	2024-10-21	9.6	CVE-2024-40084
n/a--n/a	A Buffer Overflow vulnerability in the local_app_set_router_wan function of Vilo 5 Mesh WiFi System <= 5.16.1.33 allows remote, unauthenticated attackers to execute arbitrary code via pppoe_username and pppoe_password fields being larger than 128 bytes in length.	2024-10-21	9.6	CVE-2024-40085
n/a--n/a	A Buffer Overflow vulnerability in the local_app_set_router_wifi_SSID_PWD function of Vilo 5 Mesh WiFi System <= 5.16.1.33 allows remote, unauthenticated attackers to execute arbitrary code via a password field larger than 64 bytes in length.	2024-10-21	9.6	CVE-2024-40086
n/a--n/a	Vilo 5 Mesh WiFi System <= 5.16.1.33 is vulnerable to Insecure Permissions. Lack of authentication in the custom TCP service on port 5432 allows remote, unauthenticated attackers to gain administrative access over the router.	2024-10-21	9.6	CVE-2024-40087
n/a--n/a	A Command Injection vulnerability in Vilo 5 Mesh WiFi System <= 5.16.1.33 allows remote, authenticated attackers to execute arbitrary code by injecting shell commands into the name of the Vilo device.	2024-10-21	9.1	CVE-2024-40089
n/a--n/a	Buffer Overflow in coap_msg.c in FreeCoAP allows remote attackers to execute arbitrary code or cause a denial of service (stack buffer overflow) via a crafted packet.	2024-10-22	9.8	CVE-2024-40494
n/a--n/a	HTMLDOC v1.9.18 contains a buffer overflow in parse_pre function,ps-pdf.cxx:5681.	2024-10-24	9.8	CVE-2024-46478
n/a--n/a	Xlight FTP Server <3.9.4.3 has an integer overflow vulnerability in the packet parsing logic of the SFTP server, which can lead to a heap overflow with attacker-controlled content.	2024-10-22	9.8	CVE-2024-46483
n/a--n/a	A cross-site scripting (XSS) vulnerability in pfsense v2.5.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the $pconfig variable at interfaces_groups_edit.php.	2024-10-22	9.3	CVE-2024-46538
n/a--n/a	A vulnerability in the AWV (Audio, Web and Video Conferencing) component of Mitel MiCollab through 9.8 SP1 FP2 (9.8.1.201) could allow an unauthenticated attacker to conduct a SQL injection attack due to insufficient sanitization of user input. A successful exploit could allow an attacker to access non-sensitive user provisioning information and execute arbitrary SQL database commands.	2024-10-21	9.4	CVE-2024-47223
n/a--n/a	A lack of rate limiting in the OTP validation component of Digitory Multi Channel Integrated POS v1.0 allows attackers to gain access to the ordering system and place an excessive amount of food orders.	2024-10-24	9.1	CVE-2024-48143
n/a--n/a	SQL injection vulnerability in Hanzhou Haobo network management system 1.0 allows a remote attacker to execute arbitrary code via a crafted script.	2024-10-25	9.8	CVE-2024-48204
n/a--n/a	Learning with Texts (LWT) 2.0.3 is vulnerable to SQL Injection. This occurs when the application fails to properly sanitize user inputs, allowing attackers to manipulate SQL queries by injecting malicious SQL statements into URL	2024-10-21	9.8	CVE-2024-48509

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameters. By exploiting this vulnerability, an attacker could gain unauthorized access to the database, retrieve sensitive information, modify or delete data, and execute arbitrary commands.			
n/a--n/a	Incorrect access control in the firmware update and download processes of Neye3C v4.5.2.0 allows attackers to access sensitive information by analyzing the code and data within the APK file.	2024-10-24	9.8	CVE-2024-48538
n/a--n/a	Neye3C v4.5.2.0 was discovered to contain a hardcoded encryption key in the firmware update mechanism.	2024-10-24	9.8	CVE-2024-48539
n/a--n/a	The APK file in Cloud Smart Lock v2.0.1 has a leaked a URL that can call an API for binding physical devices. This vulnerability allows attackers to arbitrarily construct a request to use the app to bind to unknown devices by finding a valid serial number via a bruteforce attack.	2024-10-24	9.3	CVE-2024-48548
n/a--n/a	SQL Injection vulnerability in Best House rental management system project in php v.1.0 allows a remote attacker to execute arbitrary code via the username parameter of the login request.	2024-10-25	9.8	CVE-2024-48579
n/a--n/a	SQL Injection vulnerability in Best courier management system in php v.1.0 allows a remote attacker to execute arbitrary code via the email parameter of the login request.	2024-10-25	9.8	CVE-2024-48580
n/a--n/a	File Upload vulnerability in Best courier management system in php v.1.0 allows a remote attacker to execute arbitrary code via the admin_class.php component.	2024-10-25	9.8	CVE-2024-48581
n/a--n/a	An issue in DCME-320-L <=9.3.2.114 allows a remote attacker to execute arbitrary code via the log_u_umount.php component.	2024-10-21	9.8	CVE-2024-48659
n/a--n/a	A Local Privilege Escalation issue was discovered in Y Soft SAFEQ 6 Build 53. The SafeQ JMX service running on port 9696 is vulnerable to JMX MLet attacks. Because the service did not enforce authentication and was running under the "NT Authority\System" user, an attacker is able to use the vulnerability to execute arbitrary code and elevate to the system user.	2024-10-22	8.4	CVE-2022-23862
n/a--n/a	An issue in the server_handle_regular function of the test_coap_server.c file within the FreeCoAP project allows remote attackers to cause a Denial of Service through specially crafted packets.	2024-10-22	8.2	CVE-2024-31029
n/a--n/a	A lack of input validation in Realtek SD card reader driver before 10.0.26100.21374 through the implementation of the IOCTL_SCSI_PASS_THROUGH control of the SD card reader driver allows an attacker to write to predictable kernel memory locations, even as a low-privileged user.	2024-10-23	8.8	CVE-2024-40431
n/a--n/a	A vulnerability in the Web Interface component of Mitel MiCollab through 9.8 SP1 (9.8.1.5) and MiVoice Business Solution Virtual Instance (MiVB SVI) through 1.0.0.27 could allow an authenticated attacker to conduct a command injection attack, due to insufficient parameter sanitization. A successful exploit could allow an attacker to execute arbitrary commands with elevated privileges within the context of the system.	2024-10-21	8.8	CVE-2024-41714
n/a--n/a	An arbitrary file upload vulnerability in the Ticket Generation function of Ladybird Web Solution Faveo-Helpdesk v2.0.3 allows attackers to execute arbitrary code via uploading a crafted .html or .svg file.	2024-10-22	8.2	CVE-2024-46482
n/a--n/a	A vulnerability in the AWV (Audio, Web, and Video) Conferencing component of Mitel MiCollab through 9.8 SP1 FP2 (9.8.1.201) could allow an unauthenticated attacker to perform unauthorized data-access attacks due to missing	2024-10-21	8.2	CVE-2024-47912

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authentication mechanisms. A successful exploit could allow an attacker to access and delete sensitive information.			
n/a--n/a	Shenzhen Tuoshi Network Communications Co.,Ltd 5G CPE Router NR500-EA RG500UEAABxCOMSLICv3.2.2543.12.18 was discovered to contain a command injection vulnerability via the component at_command.asp.	2024-10-24	8.8	CVE-2024-48440
n/a--n/a	Wuhan Tianyu Information Industry Co., Ltd Tianyu CPE Router CommonCPExCPETS_v3.2.468.11.04_P4 was discovered to contain a command injection vulnerability via the component at_command.asp.	2024-10-24	8.8	CVE-2024-48441
n/a--n/a	Incorrect access control in the firmware update and download processes of Ruochan Smart v4.4.7 allows attackers to access sensitive information by analyzing the code and data within the APK file.	2024-10-24	8.4	CVE-2024-48541
n/a--n/a	Incorrect access control in the firmware update and download processes of Yamaha Headphones Controller v1.6.7 allows attackers to access sensitive information by analyzing the code and data within the APK file.	2024-10-24	8.4	CVE-2024-48542
n/a--n/a	Incorrect access control in the firmware update and download processes of Sylvania Smart Home v3.0.3 allows attackers to access sensitive information by analyzing the code and data within the APK file.	2024-10-24	8.4	CVE-2024-48544
n/a--n/a	Incorrect access control in the firmware update and download processes of IVY Smart v4.5.0 allows attackers to access sensitive information by analyzing the code and data within the APK file.	2024-10-24	8.4	CVE-2024-48545
n/a--n/a	Incorrect access control in the firmware update and download processes of Wear Sync v1.2.0 allows attackers to access sensitive information by analyzing the code and data within the APK file.	2024-10-24	8.4	CVE-2024-48546
n/a--n/a	Incorrect access control in the firmware update and download processes of DreamCatcher Life v1.8.7 allows attackers to access sensitive information by analyzing the code and data within the APK file.	2024-10-24	8.4	CVE-2024-48547
n/a--n/a	Online Clinic Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /success/editp.php?action=edit.	2024-10-21	8.1	CVE-2024-48597
n/a--n/a	A vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab through 9.8 SP1 FP2 (9.8.1.201) could allow an unauthenticated attacker to conduct a path traversal attack, due to insufficient input validation. A successful exploit could allow unauthorized access, enabling the attacker to view, corrupt, or delete users' data and system configurations.	2024-10-21	7.5	CVE-2024-41713
n/a--n/a	Integer Overflow in fast_ping.c in SmartDNS Release46 allows remote attackers to cause a Denial of Service via misaligned memory access.	2024-10-22	7.5	CVE-2024-42643
n/a--n/a	Incorrect Access Control in GStreamer RTSP server 1.25.0 in gst-rtsp-server/rtsp-media.c allows remote attackers to cause a denial of service via a series of specially crafted hexstream requests.	2024-10-22	7.5	CVE-2024-44331
n/a--n/a	An issue was discovered in Zimbra Collaboration (ZCS) 10.1.x before 10.1.1, 10.0.x before 10.0.9, 9.0.0 before Patch 41, and 8.8.15 before Patch 46. It allows authenticated users to exploit Server-Side Request Forgery (SSRF) due to improper input sanitization and misconfigured domain whitelisting. This issue permits unauthorized HTTP requests to be sent to internal services, which can lead to Remote Code Execution (RCE) by chaining Command Injection within the internal service. When combined with existing XSS vulnerabilities, this SSRF issue can further facilitate Remote Code Execution (RCE).	2024-10-22	7.5	CVE-2024-45518

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	A prompt injection vulnerability in the chatbox of Blackbox AI v1.3.95 allows attackers to access and exfiltrate all previous and subsequent chat data between the user and the AI assistant via a crafted message.	2024-10-24	7.5	CVE-2024-48139
n/a--n/a	A prompt injection vulnerability in the chatbox of Butterfly Effect Limited Monica Your AI Copilot powered by ChatGPT4 v6.3.0 allows attackers to access and exfiltrate all previous and subsequent chat data between the user and the AI assistant via a crafted message.	2024-10-24	7.5	CVE-2024-48140
n/a--n/a	A prompt injection vulnerability in the chatbox of Zhipu AI CodeGeeX v2.17.0 allows attackers to access and exfiltrate all previous and subsequent chat data between the user and the AI assistant via a crafted message.	2024-10-24	7.5	CVE-2024-48141
n/a--n/a	A prompt injection vulnerability in the chatbox of Butterfly Effect Limited Monica ChatGPT AI Assistant v2.4.0 allows attackers to access and exfiltrate all previous and subsequent chat data between the user and the AI assistant via a crafted message.	2024-10-24	7.5	CVE-2024-48142
n/a--n/a	Funadmin 5.0.2 is vulnerable to SQL Injection via the selectFields parameter in the index method of \backend\controller\auth\Auth.php.	2024-10-21	7.2	CVE-2024-48231
n/a--n/a	An issue in SourceCodester Purchase Order Management System v1.0 allows a remote attacker to execute arbitrary code via the /admin?page=user component	2024-10-24	7.2	CVE-2024-48454
n/a--n/a	An issue in Helakuru Desktop Application v1.1 allows a local attacker to execute arbitrary code via the lack of proper validation of the wow64log.dll file.	2024-10-22	7.8	CVE-2024-48605
n/a--n/a	In Minecraft mod "Command Block IDE" up to and including version 0.4.9, a missing authorization (CWE-862) allows any user to modify "function" files used by the game when installed on a dedicated server.	2024-10-21	7.5	CVE-2024-48645
NVIDIA--GPU, vGPU, and Cloud Gaming	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability which could allow a privileged attacker to escalate permissions. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-10-26	8.2	CVE-2024-0126
NVIDIA--GPU, vGPU, and Cloud Gaming	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-10-26	7.8	CVE-2024-0117
NVIDIA--GPU, vGPU, and Cloud Gaming	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-10-26	7.8	CVE-2024-0118
NVIDIA--GPU, vGPU, and Cloud Gaming	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-10-26	7.8	CVE-2024-0119
NVIDIA--GPU, vGPU, and Cloud Gaming	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-10-26	7.8	CVE-2024-0120
NVIDIA--GPU, vGPU, and Cloud Gaming	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-10-26	7.8	CVE-2024-0121

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NVIDIA--vGPU and Cloud Gaming	NVIDIA vGPU software contains a vulnerability in the GPU kernel driver of the vGPU Manager for all supported hypervisors, where a user of the guest OS can cause an improper input validation by compromising the guest OS kernel. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	2024-10-26	7.8	CVE-2024-0127
NVIDIA--vGPU and Cloud Gaming	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager that allows a user of the guest OS to access global resources. A successful exploit of this vulnerability might lead to information disclosure, data tampering, and escalation of privileges.	2024-10-26	7.1	CVE-2024-0128
Okta--Okta Verify for iOS	A vulnerability in Okta Verify for iOS versions 9.25.1 (beta) and 9.27.0 (including beta) allows push notification responses through the iOS ContextExtension feature allowing the authentication to proceed regardless of the user's selection. When a user long-presses the notification banner and selects an option, both options allow the authentication to succeed. The ContextExtension feature is one of several push mechanisms available when using Okta Verify Push on iOS devices. The vulnerable flows include: * When a user is presented with a notification on a locked screen, the user presses on the notification directly and selects their reply without unlocking the device; * When a user is presented with a notification on the home screen and drags the notification down and selects their reply; * When an Apple Watch is used to reply directly to a notification. A pre-condition for this vulnerability is that the user must have enrolled in Okta Verify while the Okta customer was using Okta Classic. This applies irrespective of whether the organization has since upgraded to Okta Identity Engine.	2024-10-24	8.1	CVE-2024-10327
OpenRefine--OpenRefine	OpenRefine is a free, open source tool for working with messy data. Prior to version 3.8.3, the `/extension/gdata/authorized` endpoint includes the `state` GET parameter verbatim in a `<script>` tag in the output, so without escaping. An attacker could lead or redirect a user to a crafted URL containing JavaScript code, which would then cause that code to be executed in the victim's browser as if it was part of OpenRefine. Version 3.8.3 fixes this issue.	2024-10-24	8.1	CVE-2024-47878
OpenRefine--OpenRefine	OpenRefine is a free, open source tool for working with messy data. Prior to version 3.8.3, the `export-rows` command can be used in such a way that it reflects part of the request verbatim, with a Content-Type header also taken from the request. An attacker could lead a user to a malicious page that submits a form POST that contains embedded JavaScript code. This code would then be included in the response, along with an attacker-controlled `Content-Type` header, and so potentially executed in the victim's browser as if it was part of OpenRefine. The attacker-provided code can do anything the user can do, including deleting projects, retrieving database passwords, or executing arbitrary Jython or Closure expressions, if those extensions are also present. The attacker must know a valid project ID of a project that contains at least one row. Version 3.8.3 fixes the issue.	2024-10-24	8.1	CVE-2024-47880
OpenRefine--OpenRefine	OpenRefine is a free, open source tool for working with messy data. Starting in version 3.4-beta and prior to version 3.8.3, in the `database` extension, the "enable_load_extension" property can be set for the SQLite integration, enabling an attacker to load (local or remote) extension DLLs and so run arbitrary code on the server. The attacker needs to have network access to the OpenRefine instance. Version 3.8.3 fixes this issue.	2024-10-24	8.1	CVE-2024-47881
OpenRefine--OpenRefine	OpenRefine is a free, open source tool for working with messy data. Prior to version 3.8.3, lack of cross-site request forgery protection on the `preview-expression` command means that visiting a malicious website could cause an attacker-controlled expression to be executed. The expression can contain arbitrary Clojure or Python code. The attacker must know a valid project ID of a project that contains at least one row, and the attacker must convince the victim to open a malicious webpage. Version 3.8.3 fixes the issue.	2024-10-24	7.6	CVE-2024-47879

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
OpenRefine--OpenRefine	OpenRefine is a free, open source tool for working with messy data. The load-language command expects a `lang` parameter from which it constructs the path of the localization file to load, of the form `translations-$LANG.json`. But when doing so in versions prior to 3.8.3, it does not check that the resulting path is in the expected directory, which means that this command could be exploited to read other JSON files on the file system. Version 3.8.3 addresses this issue.	2024-10-24	7.1	CVE-2024-49760
OpenRefine--simile-butterfly	The OpenRefine fork of the MIT Simile Butterfly server is a modular web application framework. The Butterfly framework uses the `java.net.URL` class to refer to (what are expected to be) local resource files, like images or templates. This works: "opening a connection" to these URLs opens the local file. However, prior to version 1.2.6, if a `file:/` URL is directly given where a relative path (resource name) is expected, this is also accepted in some code paths; the app then fetches the file, from a remote machine if indicated, and uses it as if it was a trusted part of the app's codebase. This leads to multiple weaknesses and potential weaknesses. An attacker that has network access to the application could use it to gain access to files, either on the the server's filesystem (path traversal) or shared by nearby machines (server-side request forgery with e.g. SMB). An attacker that can lead or redirect a user to a crafted URL belonging to the app could cause arbitrary attacker-controlled JavaScript to be loaded in the victim's browser (cross-site scripting). If an app is written in such a way that an attacker can influence the resource name used for a template, that attacker could cause the app to fetch and execute an attacker-controlled template (remote code execution). Version 1.2.6 contains a patch.	2024-10-24	9.1	CVE-2024-47883
pandorafms -- pandora_fms	A post-authentication arbitrary file read vulnerability within the server plugins section in plugin edition feature. This issue affects Pandora FMS: from 700 through <777.3.	2024-10-22	8.8	CVE-2024-35308
pandorafms -- pandora_fms	A post-authentication SQL Injection vulnerability within the filters parameter of the extensions/agents_modules_csv functionality. This issue affects Pandora FMS: from 700 through <777.3.	2024-10-22	8.8	CVE-2024-9987
phpgurukul -- client_management_system	Client Management System 1.0 was discovered to contain a SQL injection vulnerability via the Between Dates Reports parameter at /admin/bwdates-reports-ds.php.	2024-10-22	7.5	CVE-2024-48570
phpgurukul -- medical_card_generation_system	A vulnerability classified as critical has been found in PHPGurukul Medical Card Generation System 1.0. This affects an unknown part of the file /admin/edit-card-detail.php of the component Managecard Edit Card Detail Page. The manipulation of the argument editid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-23	7.2	CVE-2024-10298
phpgurukul -- medical_card_generation_system	A vulnerability classified as critical was found in PHPGurukul Medical Card Generation System 1.0. This vulnerability affects unknown code of the file /admin/view-card-detail.php of the component Managecard View Detail Page. The manipulation of the argument viewid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-23	7.2	CVE-2024-10299
phpgurukul -- medical_card_generation_system	A vulnerability, which was classified as critical, has been found in PHPGurukul Medical Card Generation System 1.0. This issue affects some unknown processing of the file /admin/view-enquiry.php of the component View Enquiry Page. The manipulation of the argument viewid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-23	7.2	CVE-2024-10300
phpgurukul -- medical_card_generation_system	A vulnerability, which was classified as critical, was found in PHPGurukul Medical Card Generation System 1.0. Affected is an unknown function of the file /admin/search-medicalcard.php of the component Search. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-23	7.2	CVE-2024-10301

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
princelycesar -- hospital_management_system	SQL Injection vulnerability in hospital management system in php with source code v.1.0.0 allows a remote attacker to execute arbitrary code.	2024-10-22	7.2	CVE-2024-48657
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2024.0.0, an Authentication Bypass issue exists which allows an attacker to obtain encrypted user credentials.	2024-10-24	9.8	CVE-2024-7763
properfraction -- profilepress	The ProfilePress Pro plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 4.11.1. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not have an already-existing account for the service returning the token.	2024-10-23	9.8	CVE-2024-9947
pyload--pyload	pyLoad is a free and open-source Download Manager. The folder `/.pyload/scripts` has scripts which are run when certain actions are completed, for e.g. a download is finished. By downloading a executable file to a folder in /scripts and performing the respective action, remote code execution can be achieved in versions prior to 0.5.0b3.dev87. A file can be downloaded to such a folder by changing the download folder to a folder in `/scripts` path and using the `/flashgot` API to download the file. This vulnerability allows an attacker with access to change the settings on a pyload server to execute arbitrary code and completely compromise the system. Version 0.5.0b3.dev87 fixes this issue.	2024-10-25	9.1	CVE-2024-47821
Qode Interactive--Qi Blocks	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Qode Interactive Qi Blocks.This issue affects Qi Blocks: from n/a through 1.3.2.	2024-10-23	7.5	CVE-2024-49690
Red Hat--Red Hat Enterprise Linux 6	A use-after-free vulnerability was found in the QEMU LSI53C895A SCSI Host Bus Adapter emulation. This issue can lead to a crash or VM escape.	2024-10-21	8.2	CVE-2024-6519
Red Hat--Red Hat Enterprise Linux 7.7 Advanced Update Support	A flaw was found in the libreswan client plugin for NetworkManager (NetkworkManager-libreswan), where it fails to properly sanitize the VPN configuration from the local unprivileged user. In this configuration, composed by a key-value format, the plugin fails to escape special characters, leading the application to interpret values as keys. One of the most critical parameters that could be abused by a malicious user is the `leftupdown`key. This key takes an executable command as a value and is used to specify what executes as a callback in NetworkManager-libreswan to retrieve configuration settings back to NetworkManager. As NetworkManager uses Polkit to allow an unprivileged user to control the system's network configuration, a malicious actor could achieve local privilege escalation and potential code execution as root in the targeted machine by creating a malicious configuration.	2024-10-22	7.8	CVE-2024-9050
ReneeCussack--3D Work In Progress	Unrestricted Upload of File with Dangerous Type vulnerability in ReneeCussack 3D Work In Progress allows Upload a Web Shell to a Web Server.This issue affects 3D Work In Progress: from n/a through 1.0.3.	2024-10-23	9.9	CVE-2024-49652
ReneeCussack--3D Work In Progress	Missing Authorization vulnerability in ReneeCussack 3D Work In Progress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects 3D Work In Progress: from n/a through 1.0.3.	2024-10-23	7.7	CVE-2024-49657
Revmakx--Backup and Staging by WP Time Capsule	Deserialization of Untrusted Data vulnerability in Revmakx Backup and Staging by WP Time Capsule allows Object Injection.This issue affects Backup and Staging by WP Time Capsule: from n/a through 1.22.21.	2024-10-23	7.2	CVE-2024-49684

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Rockwell Automation--FactoryTalk ThinManager	CVE-2024-10386 IMPACT An authentication vulnerability exists in the affected product. The vulnerability could allow a threat actor with network access to send crafted messages to the device, potentially resulting in database manipulation.	2024-10-25	9.8	CVE-2024-10386
Rockwell Automation--FactoryTalk ThinManager	CVE-2024-10387 IMPACT A Denial-of-Service vulnerability exists in the affected product. The vulnerability could allow a threat actor with network access to send crafted messages to the device, potentially resulting in Denial-of-Service.	2024-10-25	7.5	CVE-2024-10387
roveridx -- rover_idx	The Rover IDX plugin for WordPress is vulnerable to Authentication Bypass in versions up to, and including, 3.0.0.2905. This is due to insufficient validation and capability check on the 'rover_idx_refresh_social_callback' function. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to log in to administrator. The vulnerability is partially patched in version 3.0.0.2905 and fully patched in version 3.0.0.2906.	2024-10-22	8.8	CVE-2024-10002
sangoma -- asterisk	An issue was discovered in Sangoma Asterisk through 18.20.0, 19.x and 20.x through 20.5.0, and 21.x through 21.0.0, and Certified Asterisk through 18.9-cert5. In manager.c, the functions action_getconfig() and action_getconfigJson() do not process the input file path, resulting in a path traversal vulnerability. In versions without the restrictedFile() function, no processing is done on the input path. In versions with the restrictedFile() function, path traversal is not processed.	2024-10-21	7.8	CVE-2024-49215
Sharp Corporation--Sharp Digital Full-color MFPs and Monochrome MFPs	Sharp and Toshiba Tec MFPs improperly process HTTP authentication requests, resulting in an authentication bypass vulnerability.	2024-10-25	9.1	CVE-2024-47406
Sharp Corporation--Sharp Digital Full-color MFPs and Monochrome MFPs	Sharp and Toshiba Tec MFPs provide configuration related APIs. They are expected to be called by administrative users only, but insufficiently restricted. A non-administrative user may execute some configuration APIs.	2024-10-25	8.1	CVE-2024-47005
Sharp Corporation--Sharp Digital Full-color MFPs and Monochrome MFPs	Sharp and Toshiba Tec MFPs contain multiple Out-of-bounds Read vulnerabilities, due to improper processing of keyword search input and improper processing of SOAP messages. Crafted HTTP requests may cause affected products crashed.	2024-10-25	7.5	CVE-2024-42420
Sharp Corporation--Sharp Digital Full-color MFPs and Monochrome MFPs	Sharp and Toshiba Tec MFPs improperly process HTTP request headers, resulting in an Out-of-bounds Read vulnerability. Crafted HTTP requests may cause affected products crashed.	2024-10-25	7.5	CVE-2024-43424
Sharp Corporation--Sharp Digital Full-	Sharp and Toshiba Tec MFPs improperly process query parameters in HTTP requests, which may allow contamination of unintended data to HTTP response	2024-10-25	7.4	CVE-2024-47549

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
color MFPs and Monochrome MFPs	headers. Accessing a crafted URL which points to an affected product may cause malicious script executed on the web browser.			
Sharp Corporation--Sharp Digital Full-color MFPs and Monochrome MFPs	Sharp and Toshiba Tec MFPs improperly process query parameters in HTTP requests, resulting in a reflected cross-site scripting vulnerability. Accessing a crafted URL which points to an affected product may cause malicious script executed on the web browser.	2024-10-25	7.4	CVE-2024-47801
Siemens--InterMesh 7177 Hybrid 2.0 Subscriber	A vulnerability has been identified in InterMesh 7177 Hybrid 2.0 Subscriber (All versions < V8.2.12), InterMesh 7707 Fire Subscriber (All versions < V7.2.12 only if the IP interface is enabled (which is not the default configuration)). The web server of affected devices does not sanitize the input parameters in specific GET requests that allow for code execution on operating system level. In combination with other vulnerabilities (CVE-2024-47902, CVE-2024-47903, CVE-2024-47904) this could allow an unauthenticated remote attacker to execute arbitrary code with root privileges.	2024-10-23	10	CVE-2024-47901
Siemens--InterMesh 7177 Hybrid 2.0 Subscriber	A vulnerability has been identified in InterMesh 7177 Hybrid 2.0 Subscriber (All versions < V8.2.12), InterMesh 7707 Fire Subscriber (All versions < V7.2.12 only if the IP interface is enabled (which is not the default configuration)). The web server of affected devices does not authenticate GET requests that execute specific commands (such as `ping`) on operating system level.	2024-10-23	7.2	CVE-2024-47902
Siemens--InterMesh 7177 Hybrid 2.0 Subscriber	A vulnerability has been identified in InterMesh 7177 Hybrid 2.0 Subscriber (All versions < V8.2.12), InterMesh 7707 Fire Subscriber (All versions < V7.2.12 only if the IP interface is enabled (which is not the default configuration)). The affected devices contain a SUID binary that could allow an authenticated local attacker to execute arbitrary commands with root privileges.	2024-10-23	7.8	CVE-2024-47904
skylarkcob--Extensions by HocWP Team	The Extensions by HocWP Team plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 0.2.3.2. This is due to missing validation on the user being supplied in the 'verify_email' action. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator. The vulnerability is in the Account extension.	2024-10-26	9.8	CVE-2024-9930
Snyk--Snyk Cli	The package Snyk CLI before 1.1294.0 is vulnerable to Code Injection when scanning an untrusted PHP project. The vulnerability can be triggered if Snyk test is run inside the untrusted project due to the improper handling of the current working directory name. Snyk recommends only scanning trusted projects.	2024-10-23	7.5	CVE-2024-48963
Snyk--Snyk Cli	The package Snyk CLI before 1.1294.0 is vulnerable to Code Injection when scanning an untrusted Gradle project. The vulnerability can be triggered if Snyk test is run inside the untrusted project due to the improper handling of the current working directory name. Snyk recommends only scanning trusted projects.	2024-10-23	7.5	CVE-2024-48964
SourceCodeHero--Clothes Recommendation System	A vulnerability was found in SourceCodeHero Clothes Recommendation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/index.php of the component Admin Login Page. The manipulation of the argument t1 leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-24	7.3	CVE-2024-10336
SourceCodester--Garbage Collection Management	A vulnerability was found in SourceCodester Garbage Collection Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. The exploit has been	2024-10-24	7.3	CVE-2024-10335

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
System	disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "username" to be affected. But it must be assumed that the parameter "password" is affected as well.			
SWIT--WP Sessions Time Monitoring Full Automatic	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SWIT WP Sessions Time Monitoring Full Automatic allows SQL Injection.This issue affects WP Sessions Time Monitoring Full Automatic: from n/a through 1.0.9.	2024-10-24	9.3	CVE-2024-49681
te-st -- teplobot	The TeploBot - Telegram Bot for WP plugin for WordPress is vulnerable to sensitive information disclosure due to missing authorization checks on the 'service_process' function in all versions up to, and including, 1.3. This makes it possible for unauthenticated attackers to view the Telegram Bot Token, which is a secret token to control the bot.	2024-10-22	7.3	CVE-2024-9627
Tenda--RX9 Pro	A vulnerability was found in Tenda RX9 Pro 22.03.02.20. It has been rated as critical. This issue affects the function sub_424CE0 of the file /goform/setMacFilterCfg of the component POST Request Handler. The manipulation of the argument deviceList leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-25	8.8	CVE-2024-10351
Tenda--RX9	A vulnerability classified as critical has been found in Tenda RX9 and RX9 Pro 22.03.02.10/22.03.02.20. Affected is the function sub_42EEE0 of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-23	8.8	CVE-2024-10281
Tenda--RX9	A vulnerability classified as critical was found in Tenda RX9 and RX9 Pro 22.03.02.10/22.03.02.20. Affected by this vulnerability is the function sub_42EA38 of the file /goform/SetVirtualServerCfg. The manipulation of the argument list leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-23	8.8	CVE-2024-10282
Tenda--RX9	A vulnerability, which was classified as critical, has been found in Tenda RX9 and RX9 Pro 22.03.02.20. Affected by this issue is the function sub_4337EC of the file /goform/SetNetControlList. The manipulation of the argument list leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-23	8.8	CVE-2024-10283
Theme Horse--Mags	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Theme Horse Mags.This issue affects Mags: from n/a through 1.1.6.	2024-10-23	7.5	CVE-2024-49701
total-soft -- ts_poll	The TS Poll WordPress plugin before 2.4.0 does not sanitize and escape a parameter before using it in a SQL statement, allowing admins to perform SQL injection attacks	2024-10-21	7.2	CVE-2024-8625
Trend Micro, Inc.--Trend Micro Apex One	An modOSCE SQL Injection vulnerability in Trend Micro Apex One could allow a remote attacker to execute arbitrary code on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-10-22	7.5	CVE-2024-39753
Trend Micro, Inc.--Trend Micro Cloud Edge	An command injection vulnerability in Trend Micro Cloud Edge could allow a remote attacker to execute arbitrary code on affected appliances. Please note: authentication is not required in order to exploit this vulnerability.	2024-10-22	9.8	CVE-2024-48904
Trend Micro, Inc.--Trend Micro	An improper access control vulnerability in Trend Micro Deep Security Agent 20 could allow a local attacker to escalate privileges on affected installations. Please	2024-10-22	7.8	CVE-2024-48903

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Deep Security Agent	note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.			
Trend Micro, Inc.--Trend Micro VPN (consumer)	Trend Micro VPN, version 5.8.1012 and below is vulnerable to an arbitrary file overwrite under specific conditions that can lead to elevation of privileges.	2024-10-22	7.8	CVE-2024-41183
trendmicro -- antivirus_one	Trend Micro Antivirus One versions 3.10.4 and below (Consumer) is vulnerable to an Arbitrary Configuration Update that could allow unauthorized access to product configurations and functions.	2024-10-22	7.8	CVE-2024-45334
trendmicro -- deep_discovery_inspector	A vulnerability in Trend Micro Deep Discovery Inspector (DDI) versions 5.8 and above could allow an attacker to disclose sensitive information affected installations. Please note: an attacker must first obtain the ability to execute high-privileged code (admin user rights) on the target system in order to exploit this vulnerability.	2024-10-22	9.1	CVE-2024-46902
uiuxlab--Uix Shortcodes Compatible with Gutenberg	The The Uix Shortcodes - Compatible with Gutenberg plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.9.9. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	2024-10-26	7.3	CVE-2024-9772
umbraco -- umbraco_cms	Umbraco, a free and open source .NET content management system, has a cross-site scripting vulnerability starting in version 14.0.0 and prior to versions 14.3.1 and 15.0.0. This can be leveraged to gain access to higher-privilege endpoints, e.g. if you get a user with admin privileges to run the code, you can potentially elevate all users and grant them admin privileges or access protected content. Versions 14.3.1 and 15.0.0 contain a patch. As a workaround, ensure that access to the Dictionary section is only granted to trusted users.	2024-10-22	8.7	CVE-2024-47819
Vitalii Bryl--iBryl Switch User	Authentication Bypass Using an Alternate Path or Channel vulnerability in Vitalii Bryl iBryl Switch User allows Authentication Bypass.This issue affects iBryl Switch User: from n/a through 1.0.1.	2024-10-23	8.8	CVE-2024-49675
watchtowerhq--WatchTowerHQ	The WatchTowerHQ plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.9.6. This is due to the 'watchtower_ota_token' default value is empty, and the not empty check is missing in the 'Password_Less_Access::login' function. This makes it possible for unauthenticated attackers to log in to the WatchTowerHQ client administrator user.	2024-10-26	9.8	CVE-2024-9933
WAVLINK--WN530H4	A vulnerability was found in WAVLINK WN530H4, WN530HG4 and WN572HG3 up to 20221028. It has been rated as critical. This issue affects the function set_ipv6 of the file firewall.cgi. The manipulation of the argument dhcpGateway leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-27	7.2	CVE-2024-10428
WAVLINK--WN530H4	A vulnerability classified as critical has been found in WAVLINK WN530H4, WN530HG4 and WN572HG3 up to 20221028. Affected is the function set_ipv6 of the file internet.cgi. The manipulation of the argument IPv6OpMode/IPv6IPAddr/IPv6WANIPAddr/IPv6GWAddr leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-27	7.2	CVE-2024-10429

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wellchoose -- administrative_management_system	Administrative Management System from Wellchoose does not properly validate uploaded file types, allowing remote attackers with regular privileges to upload and execute webshells.	2024-10-21	8.8	CVE-2024-10201
wellchoose -- administrative_management_system	Administrative Management System from Wellchoose has an OS Command Injection vulnerability, allowing remote attackers with regular privileges to inject and execute arbitrary OS commands.	2024-10-21	8.8	CVE-2024-10202
wellchoose -- administrative_management_system	Administrative Management System from Wellchoose has a Path Traversal vulnerability, allowing unauthenticated remote attackers to exploit this vulnerability to download arbitrary files on the server.	2024-10-21	7.5	CVE-2024-10200
Woobewoo--Product Filter by WBW	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Woobewoo Product Filter by WBW allows SQL Injection.This issue affects Product Filter by WBW: from n/a through 2.7.0.	2024-10-24	7.6	CVE-2024-49691
wpmudev--Forminator Forms Contact Form, Payment Form & Custom Form Builder	The Forminator Forms - Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on a function in all versions up to, and including, 1.35.1. This makes it possible for authenticated attackers, with Contributor-level access and above, and permissions granted by an Administrator, to create new or edit existing forms, including updating the default registration role to Administrator on User Registration forms.	2024-10-26	7.5	CVE-2024-10402
wpovernight -- woocommerce_order_proposal	The WooCommerce Order Proposal plugin for WordPress is vulnerable to privilege escalation via order proposal in all versions up to and including 2.0.5. This is due to the improper implementation of allow_payment_without_login function. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to log in to WordPress as an arbitrary user account, including administrators.	2024-10-23	7.2	CVE-2024-9927
xpeedstudio--Wp Social Login and Register Social Counter	The Wp Social Login and Register Social Counter plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 3.0.7. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not have an already-existing account for the service returning the token.	2024-10-26	9.8	CVE-2024-9501
zitadel--zitadel	The open-source identity infrastructure software Zitadel allows administrators to disable the user self-registration. Due to a missing security check in versions prior to 2.64.0, 2.63.5, 2.62.7, 2.61.4, 2.60.4, 2.59.5, and 2.58.7, disabling the "User Registration allowed" option only hid the registration button on the login page. Users could bypass this restriction by directly accessing the registration URL (/ui/login/loginname) and register a user that way. Versions 2.64.0, 2.63.5, 2.62.7, 2.61.4, 2.60.4, 2.59.5, and 2.58.7 contain a patch. No known workarounds are available.	2024-10-25	7.5	CVE-2024-49757

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
A WP Life--Contact Form Widget	Cross-Site Request Forgery (CSRF) vulnerability in A WP Life Contact Form Widget allows Cross Site Request Forgery.This issue affects Contact Form Widget: from n/a through 1.4.2.	2024-10-17	5.4	CVE-2024-48037
acronis --cyber_files	Sensitive information disclosure due to spell-jacking. The following products are affected: Acronis Cyber Files (Windows) before build 9.0.0x24.	2024-10-17	5.7	CVE-2024-49386
acronis --cyber_files	Stored cross-site scripting (XSS) vulnerability on enrollment invitation page. The following products are affected: Acronis Cyber Files (Windows) before build 9.0.0x24.	2024-10-17	4.8	CVE-2024-49392
acronis --cyber_protect	Excessive attack surface in archive-server service due to binding to an unrestricted IP address. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 38690.	2024-10-15	4.3	CVE-2024-49382
acronis --cyber_protect	Excessive attack surface in acep-importer service due to binding to an unrestricted IP address. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 38690.	2024-10-15	4.3	CVE-2024-49383
acronis --cyber_protect	Excessive attack surface in acep-collector service due to binding to an unrestricted IP address. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 38690.	2024-10-15	4.3	CVE-2024-49384
Adobe--Substance3D - Sampler	Substance3D - Sampler versions 4.5 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS) condition. An attacker could exploit this vulnerability to crash the application, resulting in a DoS. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-17	5.5	CVE-2024-47459
alimir--WP ULike All-in-One Engagement Toolkit	The WP ULike - The Ultimate Engagement Toolkit for Websites plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.7.4. This is due to missing or incorrect nonce validation on the wp_ulike_delete_history_api() function. This makes it possible for unauthenticated attackers to delete engagements via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-10-16	4.3	CVE-2024-9649
apache --cloudstack	The CloudStack Quota feature allows cloud administrators to implement a quota or usage limit system for cloud resources, and is disabled by default. In environments where the feature is enabled, due to missing access check enforcements, non-administrative CloudStack user accounts are able to access and modify quota-related configurations and data. This issue affects Apache CloudStack from 4.7.0 through 4.18.2.3; and from 4.19.0.0 through 4.19.1.1, where the Quota feature is enabled. Users are recommended to upgrade to Apache CloudStack 4.18.2.4 or 4.19.1.2, or later, which addresses this issue. Alternatively, users that do not use the Quota feature are advised to disabled the plugin by setting the global setting "quota.enable.service" to "false".	2024-10-16	6.3	CVE-2024-45461

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apintop--Add Widget After Content	The Add Widget After Content plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.4.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-10-18	4.4	CVE-2024-9892
B.M. Rafiul Alam--Awesome Contact Form7 for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in B.M. Rafiul Alam Awesome Contact Form7 for Elementor allows Stored XSS.This issue affects Awesome Contact Form7 for Elementor: from n/a through 3.0.	2024-10-17	6.5	CVE-2024-49319
Bert Kler--Movie Database	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Bert KÃ¶ÃŸler Movie Database allows Stored XSS.This issue affects Movie Database: from n/a through 1.0.11.	2024-10-18	5.9	CVE-2024-43300
blindsidenetworks--BigBlueButton	The BigBlueButton plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the the moderator code and viewer code fields in versions up to, and including, 3.0.0-beta.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with author privileges or higher to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-16	6.4	CVE-2023-7296
BogdanFix--WP SendFox	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in BogdanFix WP SendFox allows Retrieve Embedded Sensitive Data.This issue affects WP SendFox: from n/a through 1.3.1.	2024-10-17	5.3	CVE-2024-49284
bqworks--Accordion Slider	The Accordion Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'html' attribute of an accordion slider in all versions up to, and including, 1.9.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. NOTE: Successful exploitation by Contributor-level users requires an Administrator-level user to provide access to the plugin's admin area via the `Access` plugin setting, which is restricted to administrators by default.	2024-10-16	6.4	CVE-2024-9582
cert -- vince	A potential denial-of-service (DoS) vulnerability exists in CERT VINCE software versions prior to 3.0.8. An authenticated administrative user can inject an arbitrary pickle object into a user's profile, which may lead to a DoS condition when the profile is accessed. While the Django server restricts unpickling to prevent server crashes, this vulnerability could still disrupt operations.	2024-10-14	4.9	CVE-2024-9953
chertz--WP Easy Post Types	The WP Easy Post Types plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post meta in versions up to, and including, 1.4.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-18	6.4	CVE-2024-10080
Cisco--Cisco Analog Telephone Adaptor (ATA) Software	A vulnerability in the web-based management interface of Cisco ATA 190 Multiplatform Series Analog Telephone Adapter firmware could allow an authenticated, remote attacker with high privileges to execute arbitrary commands as the root user on the underlying operating system. This vulnerability is due to a lack of input sanitization in the web-based management interface. An attacker could exploit this vulnerability by sending a malicious request to the web-	2024-10-16	6.5	CVE-2024-20459

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	based management interface. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system as the root user.			
Cisco--Cisco Analog Telephone Adaptor (ATA) Software	A vulnerability in the web-based management interface of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information on an affected device.	2024-10-16	6.1	CVE-2024-20460
Cisco--Cisco Analog Telephone Adaptor (ATA) Software	A vulnerability in the CLI of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an authenticated, local attacker with high privileges to execute arbitrary commands as the root user. This vulnerability exists because CLI input is not properly sanitized. An attacker could exploit this vulnerability by sending malicious characters to the CLI. A successful exploit could allow the attacker to read and write to the underlying operating system as the root user.	2024-10-16	6	CVE-2024-20461
Cisco--Cisco Analog Telephone Adaptor (ATA) Software	A vulnerability in the web-based management interface of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an authenticated, remote attacker with low privileges to run commands as an Admin user. This vulnerability is due to incorrect authorization verification by the HTTP server. An attacker could exploit this vulnerability by sending a malicious request to the web-based management interface. A successful exploit could allow the attacker to run commands as the Admin user.	2024-10-16	5.4	CVE-2024-20420
Cisco--Cisco Analog Telephone Adaptor (ATA) Software	A vulnerability in the web-based management interface of Cisco ATA 190 Series Multiplatform Analog Telephone Adapter firmware could allow an authenticated, local attacker with low privileges to view passwords on an affected device. This vulnerability is due to incorrect sanitization of HTML content from an affected device. A successful exploit could allow the attacker to view passwords that belong to other users.	2024-10-16	5.5	CVE-2024-20462
Cisco--Cisco Analog Telephone Adaptor (ATA) Software	A vulnerability in the web-based management interface of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to modify the configuration or reboot an affected device. This vulnerability is due to the HTTP server allowing state changes in GET requests. An attacker could exploit this vulnerability by sending a malicious request to the web-based management interface on an affected device. A successful exploit could allow the attacker to make limited modifications to the configuration or reboot the device, resulting in a denial of service (DoS) condition.	2024-10-16	5.4	CVE-2024-20463
Cisco--Cisco Unified Computing System Central Software	A vulnerability in the backup feature of Cisco UCS Central Software could allow an attacker with access to a backup file to learn sensitive information that is stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method that is used for the backup function. An attacker could exploit this vulnerability by accessing a backup file and leveraging a static key that is used for the backup configuration feature. A successful exploit could allow an attacker with access to a backup file to learn sensitive information that is stored in full state backup files and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and the device SSL server certificate and key.	2024-10-16	6.3	CVE-2024-20280
Cisco--Cisco Unified Contact Center Management	A vulnerability in the web-based management interface of Cisco Unified Contact Center Management Portal (Unified CCMP) could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A	2024-10-16	6.1	CVE-2024-20512

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Portal	successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.			
code-projects--Blood Bank System	A vulnerability, which was classified as critical, was found in code-projects Blood Bank System up to 1.0. Affected is an unknown function of the file /admin/massage.php. The manipulation of the argument bid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-20	4.7	CVE-2024-10171
code-projects--Hospital Management System	A vulnerability classified as critical was found in code-projects Hospital Management System 1.0. This vulnerability affects unknown code of the file change-password.php. The manipulation of the argument cpass leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-20	6.3	CVE-2024-10169
code-projects--Hospital Management System	A vulnerability, which was classified as critical, has been found in code-projects Hospital Management System 1.0. This issue affects some unknown processing of the file get_doctor.php. The manipulation of the argument specilizationid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-20	6.3	CVE-2024-10170
code-projects--Pharmacy Management System	A vulnerability was found in code-projects Pharmacy Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /php/manage_purchase.php?action=search&tag=VOUCHER_NUMBER. The manipulation of the argument text leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-16	6.3	CVE-2024-10021
code-projects--Pharmacy Management System	A vulnerability classified as critical has been found in code-projects Pharmacy Management System 1.0. This affects an unknown part of the file /php/manage_supplier.php?action=search. The manipulation of the argument text leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-16	6.3	CVE-2024-10022
code-projects--Pharmacy Management System	A vulnerability classified as critical was found in code-projects Pharmacy Management System 1.0. This vulnerability affects unknown code of the file /php/add_new_medicine.php. The manipulation of the argument name/packing/generic_name/suppliers_name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-16	6.3	CVE-2024-10023
code-projects--Pharmacy Management System	A vulnerability, which was classified as critical, has been found in code-projects Pharmacy Management System 1.0. This issue affects some unknown processing of the file /php/manage_medicine_stock.php. The manipulation of the argument name/packing/generic_name/suppliers_name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-16	6.3	CVE-2024-10024
code-projects--Pharmacy Management System	A vulnerability was found in code-projects Pharmacy Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /manage_invoice.php. The manipulation of the argument invoice_number leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-19	6.3	CVE-2024-10136
code-projects--Pharmacy Management System	A vulnerability was found in code-projects Pharmacy Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /manage_medicine.php?action=delete. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-19	6.3	CVE-2024-10137

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--Pharmacy Management System	A vulnerability classified as critical has been found in code-projects Pharmacy Management System 1.0. Affected is an unknown function of the file /add_new_purchase.php?action=is_supplier. The manipulation of the argument name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-19	6.3	CVE-2024-10138
code-projects--Pharmacy Management System	A vulnerability classified as critical was found in code-projects Pharmacy Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /add_new_supplier.php. The manipulation of the argument name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-19	6.3	CVE-2024-10139
code-projects--Pharmacy Management System	A vulnerability, which was classified as critical, has been found in code-projects Pharmacy Management System 1.0. Affected by this issue is some unknown functionality of the file /manage_supplier.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-19	6.3	CVE-2024-10140
CodeAstrology Team--UltraAddons Elementor Lite	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CodeAstrology Team UltraAddons Elementor Lite allows Stored XSS.This issue affects UltraAddons Elementor Lite: from n/a through 1.1.8.	2024-10-17	6.5	CVE-2024-49277
codepeople--Calculated Fields Form	The Calculated Fields Form plugin for WordPress is vulnerable to HTML Injection in all versions up to, and including, 5.2.45. This is due to the plugin not properly neutralizing HTML elements from submitted forms. This makes it possible for unauthenticated attackers to inject arbitrary HTML that will render when the administrator views form submissions in their email.	2024-10-17	5.3	CVE-2024-9940
Coder426--Custom Add to Cart Button Label and Link	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Coder426 Custom Add to Cart Button Label and Link allows Stored XSS.This issue affects Custom Add to Cart Button Label and Link: from n/a through 1.6.1.	2024-10-17	6.5	CVE-2024-49296
CrossedCode--bVerse Convert	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CrossedCode bVerse Convert allows Stored XSS.This issue affects bVerse Convert: from n/a through 1.3.7.1.	2024-10-18	6.5	CVE-2024-49228
Daniele Alessandra--Da Reactions	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Daniele Alessandra Da Reactions allows Stored XSS.This issue affects Da Reactions: from n/a through 5.1.5.	2024-10-17	6.5	CVE-2024-49255
Dell--Dell OpenManage Enterprise	Dell OpenManage Enterprise, version(s) OME 4.1 and prior, contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2024-10-17	4.3	CVE-2024-45767
Dell--Secure Connect Gateway (SCG) 5.0 Appliance - SRS	Dell Secure Connect Gateway (SCG) 5.24 contains an Incorrect Default Permissions vulnerability. A local attacker with low privileges can access the file system and could potentially exploit this vulnerability to gain write access to unauthorized data and cause a version update failure condition.	2024-10-18	5.5	CVE-2024-47240
Dell--Secure Connect Gateway (SCG) 5.0	Dell Secure Connect Gateway (SCG) 5.0 Appliance - SRS, version(s) 5.24, contains an Improper Certificate Validation vulnerability. A low privileged attacker with	2024-10-18	5.5	CVE-2024-47241

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Appliance - SRS	remote access could potentially exploit this vulnerability, leading to unauthorized access and modification of transmitted data.			
Dell--Secure Connect Gateway (SCG) 5.0 Appliance - SRS	Dell Secure Connect Gateway (SCG) 5.0 Appliance - SRS, version(s) 5.24, contains a Use of a Broken or Risky Cryptographic Algorithm vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to information disclosure. The attacker may be able to use exposed credentials to access the system with privileges of the compromised account.	2024-10-18	4.6	CVE-2024-48016
dFactory--Responsive Lightbox	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in dFactory Responsive Lightbox allows Stored XSS.This issue affects Responsive Lightbox: from n/a through 2.4.8.	2024-10-17	5.9	CVE-2024-49282
DOGROW.NET--Simple Baseball Scoreboard	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in DOGROW.NET Simple Baseball Scoreboard allows Stored XSS.This issue affects Simple Baseball Scoreboard: from n/a through 1.3.	2024-10-17	6.5	CVE-2024-48025
dpdbaltics--DPD Baltic Shipping	The DPD Baltic Shipping plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'search_value' parameter in all versions up to, and including, 1.2.83 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-18	6.1	CVE-2024-9350
Eclipse Foundation--Jetty	There exists a security vulnerability in Jetty's ThreadLimitHandler.getRemote() which can be exploited by unauthorized users to cause remote denial-of-service (DoS) attack. By repeatedly sending crafted requests, attackers can trigger OutofMemory errors and exhaust the server's memory.	2024-10-14	5.9	CVE-2024-8184
Eclipse Foundation--Jetty	There exists a security vulnerability in Jetty's DosFilter which can be exploited by unauthorized users to cause remote denial-of-service (DoS) attack on the server using DosFilter. By repeatedly sending crafted requests, attackers can trigger OutofMemory errors and exhaust the server's memory finally.	2024-10-14	5.3	CVE-2024-9823
elbanyaoui--Smart Online Order for Clover	The Smart Online Order for Clover plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.5.7. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-16	6.1	CVE-2024-8787
elementinvader--ElementInvader Addons for Elementor	The ElementInvader Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's contact form widget redirect URL in all versions up to, and including, 1.2.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-16	5.4	CVE-2024-9888
elementinvader--ElementInvader Addons for Elementor	The ElementInvader Addons for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.2.9 via the Page Loader widget. This makes it possible for authenticated attackers, with contributor-level access and above, to view private/draft/password protected posts, pages, and Elementor templates that they should not have access to.	2024-10-19	4.3	CVE-2024-9889

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elementor -- website_builder	The Elementor Website Builder - More than Just a Page Builder plugin for WordPress is vulnerable to Basic Information Exposure in all versions up to, and including, 3.23.5 via the get_image_alt function. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract either excerpt data or titles of private or password-protected posts.	2024-10-15	4.3	CVE-2024-6757
EmbedThis--GoAhead	Multiple CWE-476 NULL Pointer Dereference vulnerabilities were found in GoAhead Web Server up to version 6.0.0 when compiled with the ME_GOAHEAD_REPLACE_MALLOC flag. Without a memory notifier for allocation failures, remote attackers can exploit these vulnerabilities by sending malicious requests, leading to a crash and Denial of Service (DoS).	2024-10-17	5.9	CVE-2024-3184
EmbedThis--GoAhead	CWE-476 NULL Pointer Dereference vulnerability in the evalExpr() function of GoAhead Web Server (version <= 6.0.0) when compiled with the ME_GOAHEAD_JAVASCRIPT flag. This vulnerability allows a remote attacker with the privileges to modify JavaScript template (JST) files to trigger a crash and cause a Denial of Service (DoS) by providing malicious templates.	2024-10-17	5.3	CVE-2024-3186
EmbedThis--GoAhead	This issue tracks two CWE-416 Use After Free (UAF) and one CWE-415 Double Free vulnerabilities in Goahead versions <= 6.0.0. These are caused by JST values not being nulled when freed during parsing of JST templates. If the ME_GOAHEAD_JAVASCRIPT flag is enabled, a remote attacker with the privileges to modify JavaScript template (JST) files could exploit this by providing malicious templates. This may lead to memory corruption, potentially causing a Denial of Service (DoS) or, in rare cases, code execution, though the latter is highly context-dependent.	2024-10-17	5.9	CVE-2024-3187
enalean -- tuleap	Tuleap is a tool for end to end traceability of application and system developments. Prior to Tuleap Community Edition 15.13.99.40, Tuleap Enterprise Edition 15.13-3, and Tuleap Enterprise Edition 15.12-6, users might receive email notification with information they should not have access to. Tuleap Community Edition 15.13.99.40, Tuleap Enterprise Edition 15.13-3, and Tuleap Enterprise Edition 15.12-6 fix this issue.	2024-10-14	5.7	CVE-2024-46988
enalean -- tuleap	Tuleap is a tool for end to end traceability of application and system developments. Prior to Tuleap Community Edition 15.13.99.37, Tuleap Enterprise Edition 15.13-3, and Tuleap Enterprise Edition 15.12-6, a site administrator could create an artifact link type with a forward label allowing them to execute uncontrolled code (or at least achieve content injection) in a mail client. Tuleap Community Edition 15.13.99.37, Tuleap Enterprise Edition 15.13-3, and Tuleap Enterprise Edition 15.12-6 fix this issue.	2024-10-14	4.8	CVE-2024-46980
enalean -- tuleap	Tuleap is a tool for end to end traceability of application and system developments. Prior to Tuleap Community Edition 15.13.99.110, Tuleap Enterprise Edition 15.13-5, and Tuleap Enterprise Edition 15.12-5, administrators of a project can access the content of trackers with permissions restrictions of project they are members of but not admin via the cross tracker search widget. Tuleap Community Edition 15.13.99.110, Tuleap Enterprise Edition 15.13-5, and Tuleap Enterprise Edition 15.12-8 fix this issue.	2024-10-14	4.9	CVE-2024-47766
enalean -- tuleap	Tuleap is a tool for end to end traceability of application and system developments. Prior to Tuleap Community Edition 15.13.99.113, Tuleap Enterprise Edition 15.13-5, and Tuleap Enterprise Edition 15.12-5, users might see tracker names they should not have access to. Tuleap Community Edition 15.13.99.113, Tuleap Enterprise Edition 15.13-5, and Tuleap Enterprise Edition 15.12-8 fix this issue.	2024-10-14	4.3	CVE-2024-47767
ESAFENET--CDG	A vulnerability was found in ESAFENET CDG 5. It has been rated as critical. Affected by this issue is the function actionPassMainApplication of the file /com/esafenet/servlet/client/MailDecryptApplicationService.java. The	2024-10-17	6.3	CVE-2024-10069

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
ESAFENET--CDG	A vulnerability classified as critical has been found in ESAFENET CDG 5. This affects the function actionPolicyPush of the file /com/esafenet/policy/action/PolicyPushControlAction.java. The manipulation of the argument policyId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-17	6.3	CVE-2024-10070
ESAFENET--CDG	A vulnerability classified as critical was found in ESAFENET CDG 5. This vulnerability affects the function actionUpdateEncryptPolicyEdit of the file /com/esafenet/servlet/policy/EncryptPolicyService.java. The manipulation of the argument encryptPolicyId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-17	6.3	CVE-2024-10071
ESAFENET--CDG	A vulnerability, which was classified as critical, has been found in ESAFENET CDG 5. This issue affects the function actionAddEncryptPolicyGroup of the file /com/esafenet/servlet/policy/EncryptPolicyService.java. The manipulation of the argument checklist leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-17	6.3	CVE-2024-10072
ESAFENET--CDG	A vulnerability has been found in ESAFENET CDG 5 and classified as critical. Affected by this vulnerability is the function updateNetSecPolicyPriority of the file /com/esafenet/servlet/ajax/NetSecPolicyAjax.java. The manipulation of the argument id/frontId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-19	6.3	CVE-2024-10133
ESAFENET--CDG	A vulnerability was found in ESAFENET CDG 5 and classified as critical. Affected by this issue is the function connectLogout of the file /com/esafenet/servlet/ajax/MultiServerAjax.java. The manipulation of the argument servername leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-19	6.3	CVE-2024-10134
ESAFENET--CDG	A vulnerability was found in ESAFENET CDG 5. It has been classified as critical. This affects the function actionDelNetSecConfig of the file /com/esafenet/servlet/netSec/NetSecConfigService.java. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-19	6.3	CVE-2024-10135
EventON--EventON Pro	The EventON PRO - WordPress Virtual Event Calendar Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.6.8. This is due to missing or incorrect nonce validation on the admin_test_email function. This makes it possible for unauthenticated attackers to send test emails to arbitrary email addresses via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-10-19	4.3	CVE-2023-6243
Exclusive Addons--Exclusive Addons Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Exclusive Addons Exclusive Addons Elementor allows Stored XSS.This issue affects Exclusive Addons Elementor: from n/a through 2.7.1.	2024-10-17	6.5	CVE-2024-49292

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
F5--BIG-IQ	A stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IQ Configuration utility that allows an attacker with the Administrator role to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-10-16	6.8	CVE-2024-47139
fahadmahmood--RSS Feed Widget	The RSS Feed Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's rfw-youtube-videos shortcode in all versions up to, and including, 2.9.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-18	6.4	CVE-2024-10057
fatcatapps--GetResponse Forms by Optin Cat	The GetResponse Forms by Optin Cat plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.5.6. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-18	6.1	CVE-2024-8740
filemanagerpro --file_manager	The File Manager Pro plugin for WordPress is vulnerable to Limited JavaScript File Upload in all versions up to, and including, 8.3.9. This is due to a lack of proper checks on allowed file types. This makes it possible for unauthenticated attackers, with permissions granted by an administrator, to upload .css and .js files, which could lead to Stored Cross-Site Scripting.	2024-10-16	5.4	CVE-2024-8918
flairNLP--flair	A vulnerability, which was classified as critical, was found in flairNLP flair 0.14.0. Affected is the function ClusteringModel of the file flair\models\clustering.py of the component Mode File Loader. The manipulation leads to code injection. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-17	5	CVE-2024-10073
flexmls--Flexmls IDX Plugin	The FlexmlsÂ® IDX Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via several parameters like 'MaxBeds' and 'MinBeds' in all versions up to, and including, 3.14.22 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-17	6.1	CVE-2024-8719
flycart--Discount Rules for WooCommerce Create Smart WooCommerce Coupons & Discounts, Bulk Discount, BOGO Coupons	The Discount Rules for WooCommerce plugin for WordPress is vulnerable to missing authorization via several AJAX actions in versions up to, and including, 2.0.2 due to missing capability checks on various functions. This makes it possible for subscriber-level attackers to execute various actions and perform a wide variety of actions such as modifying rules and saving configurations.	2024-10-16	6.3	CVE-2020-36834
flycart--Discount Rules for WooCommerce Create Smart WooCommerce Coupons & Discounts, Bulk Discount, BOGO	The Discount Rules for WooCommerce - Create Smart WooCommerce Coupons & Discounts, Bulk Discount, BOGO Coupons plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.6.5. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a site administrator into performing an action such as clicking on a link. Please note that this is only	2024-10-16	4.7	CVE-2024-8541

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Coupons	exploitable when the 'Leave a Review' notice is present, which occurs after 100 orders are made and disappears after a user dismisses the notice.			
gantry--Gantry 4 Framework	The Gantry 4 Framework plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'override_id' parameter in all versions up to, and including, 4.1.21 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-18	6.1	CVE-2024-9382
giuliopanda--Bulk images optimizer: Resize, optimize, convert to webp, rename	The Bulk images optimizer: Resize, optimize, convert to webp, rename â€¦ plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_configuration' function in all versions up to, and including, 2.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update plugin options.	2024-10-18	4.3	CVE-2024-9361
google -- chrome	Inappropriate implementation in Navigations in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	2024-10-15	5.3	CVE-2024-9966
google -- chrome	Inappropriate implementation in PictureInPicture in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	4.3	CVE-2024-9958
google -- chrome	Inappropriate implementation in Permissions in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	4.3	CVE-2024-9962
google -- chrome	Insufficient data validation in Downloads in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	4.3	CVE-2024-9963
google -- chrome	Inappropriate implementation in Payments in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Low)	2024-10-15	4.3	CVE-2024-9964
Gora Tech LLC--Cooked Pro	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Gora Tech LLC Cooked Pro allows Stored XSS.This issue affects Cooked Pro: from n/a before 1.8.0.	2024-10-17	6.5	CVE-2024-49289
Gora Tech LLC--Cooked Pro	Cross-Site Request Forgery (CSRF) vulnerability in Gora Tech LLC Cooked Pro allows Cross Site Request Forgery.This issue affects Cooked Pro: from n/a before 1.8.0.	2024-10-20	4.3	CVE-2024-49290
Hafiz Uddin Ahmed--Crazy Call To Action Box	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hafiz Uddin Ahmed Crazy Call To Action Box allows Stored XSS.This issue affects Crazy Call To Action Box: from n/a through 1.0.5.	2024-10-18	6.5	CVE-2024-49236
Hans Matzen--wp-Monalisa	Cross-Site Request Forgery (CSRF) vulnerability in Hans Matzen wp-Monalisa allows Cross Site Request Forgery.This issue affects wp-Monalisa: from n/a through 6.4.	2024-10-17	4.3	CVE-2024-48038

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Harpreet Singh--Ajax Custom CSS/JS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Harpreet Singh Ajax Custom CSS/JS allows Reflected XSS.This issue affects Ajax Custom CSS/JS: from n/a through 2.0.4.	2024-10-18	6.5	CVE-2024-49230
HashThemes--Smart Blocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HashThemes Smart Blocks allows Stored XSS.This issue affects Smart Blocks: from n/a through 2.0.	2024-10-16	6.5	CVE-2024-49270
hcltech -- bigfix_platform	A dynamic search for a prerequisite library could allow the possibility for an attacker to replace the correct file under some circumstances.	2024-10-14	5.3	CVE-2024-30117
heateor--Social Sharing Plugin Sassy Social Share	The Sassy Social Share plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'urls' parameter called via the 'heateor_sss_sharing_count' AJAX action in versions up to, and including, 3.3.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-16	6.1	CVE-2022-4971
HFO4--shudong-share	A vulnerability classified as critical has been found in HFO4 shudong-share up to 2.4.7. This affects an unknown part of the file /includes/create_share.php of the component Share Handler. The manipulation of the argument fkey leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-18	6.3	CVE-2024-10129
honojs--hono	Hono, a web framework, prior to version 4.6.5 is vulnerable to bypass of cross-site request forgery (CSRF) middleware by a request without Content-Type header. Although the CSRF middleware verifies the Content-Type Header, Hono always considers a request without a Content-Type header to be safe. This can allow an attacker to bypass CSRF protection implemented with Hono CSRF middleware. Version 4.6.5 fixes this issue.	2024-10-15	5.9	CVE-2024-48913
HT Plugins--WP Education	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HT Plugins WP Education allows Stored XSS.This issue affects WP Education: from n/a through 1.2.8.	2024-10-20	6.5	CVE-2024-49630
IBM--Watson Studio Local	IBM Watson Studio Local 1.2.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	2024-10-16	4.3	CVE-2024-49340
IBM--WebSphere Application Server	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-10-16	5.5	CVE-2024-45071
IBM--WebSphere Application Server	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A privileged user could exploit this vulnerability to expose sensitive information or consume memory resources.	2024-10-16	5.5	CVE-2024-45072
IBM--WebSphere Application Server	IBM WebSphere Application Server 8.5 is vulnerable to a denial of service, under certain configurations, caused by an unexpected specially crafted request. A remote attacker could exploit this vulnerability to cause an error resulting in a denial of service.	2024-10-15	5.9	CVE-2024-45085
india-web-developer--SEO	The SEO Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post meta in versions up to, and including, 1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible	2024-10-16	6.4	CVE-2024-9521

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Manager	for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
Infomaniak Staff--VOD Infomaniak	Cross-Site Request Forgery (CSRF) vulnerability in Infomaniak Staff VOD Infomaniak allows Cross Site Request Forgery.This issue affects VOD Infomaniak: from n/a through 1.5.7.	2024-10-20	5.4	CVE-2024-49274
ioannup--Edit WooCommerce Templates	The Edit WooCommerce Templates plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-18	6.1	CVE-2024-10049
Javier Loureiro--El mejor Cluster	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Javier Loureiro El mejor Cluster allows DOM-Based XSS.This issue affects El mejor Cluster: from n/a through 1.1.14.	2024-10-18	6.5	CVE-2024-49232
JetBrains--Ktor	In JetBrains Ktor before 3.0.0 improper caching in HttpCache Plugin could lead to response information disclosure	2024-10-17	5.3	CVE-2024-49580
k2servicecom--Product Customizer Light	The Product Customizer Light plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-18	6.4	CVE-2024-9848
Kubernetes--Image Builder	A security issue was discovered in the Kubernetes Image Builder versions <= v0.1.37 where default credentials are enabled during the image build process when using the Nutanix, OVA, QEMU or raw providers. The credentials can be used to gain root access. The credentials are disabled at the conclusion of the image build process. Kubernetes clusters are only affected if their nodes use VM images created via the Image Builder project. Because these images were vulnerable during the image build process, they are affected only if an attacker was able to reach the VM where the image build was happening and used the vulnerability to modify the image at the time the image build was occurring.	2024-10-15	6.3	CVE-2024-9594
leap13--Premium Addons for Elementor	The Premium Addons for Elementor plugin for WordPress is vulnerable to Arbitrary Option Updates in versions up to, and including, 4.5.1. This is due to missing capability and nonce checks in the pa_dismiss_admin_notice AJAX action. This makes it possible for authenticated subscriber+ attackers to change arbitrary options with a restricted value of 1 on vulnerable WordPress sites.	2024-10-16	6.5	CVE-2021-4445
Limb--WordPress Gallery Plugin Limb Image Gallery	Path Traversal: '.../...//' vulnerability in Limb WordPress Gallery Plugin - Limb Image Gallery.This issue affects WordPress Gallery Plugin - Limb Image Gallery: from n/a through 1.5.7.	2024-10-16	6.5	CVE-2024-49258
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: mm: avoid leaving partial pfn mappings around in error case As Jann points out, PFN mappings are special, because unlike normal memory mappings, there is no lifetime information associated with the mapping - it is just a raw mapping of PFNs with no reference counting of a 'struct page'. That's all very much intentional, but it does mean that it's easy to mess up the cleanup in case of errors. Yes, a failed mmap() will always eventually clean up any partial mappings, but without any explicit lifetime in the page table mapping itself, it's very easy to do the error handling in the wrong order. In particular, it's easy to mistakenly free the physical backing store before the page tables are actually cleaned up and (temporarily)	2024-10-15	5.5	CVE-2024-47674

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	have stale dangling PTE entries. To make this situation less error-prone, just make sure that any partial pfn mapping is torn down early, before any other error handling.			
lolitaframework--Branding	The Branding plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-18	6.4	CVE-2024-9452
LOOS,Inc.--Arkhe Blocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LOOS,Inc. Arkhe Blocks allows Stored XSS.This issue affects Arkhe Blocks: from n/a through 2.23.0.	2024-10-17	6.5	CVE-2024-49261
madrasthemes--MAS Companies For WP Job Manager	The MAS Companies For WP Job Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.0.13. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-18	6.1	CVE-2024-9206
MadrasThemes--MAS Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MadrasThemes MAS Elementor allows DOM-Based XSS.This issue affects MAS Elementor: from n/a through 1.1.6.	2024-10-18	6.5	CVE-2024-49233
Martin Gibson--IdeaPush	Cross-Site Request Forgery (CSRF) vulnerability in Martin Gibson IdeaPush allows Cross Site Request Forgery.This issue affects IdeaPush: from n/a through 8.69.	2024-10-20	4.3	CVE-2024-49275
maxfoundry--WordPress Social Share Buttons	The WordPress Social Share Buttons plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.19. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-19	6.1	CVE-2024-9219
Md Abdul Kader--Easy Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Md Abdul Kader Easy Addons for Elementor allows Stored XSS.This issue affects Easy Addons for Elementor: from n/a through 1.3.0.	2024-10-20	6.5	CVE-2024-49631
Michael Tran--Table of Contents Plus	Cross-Site Request Forgery (CSRF) vulnerability in Michael Tran Table of Contents Plus allows Cross Site Request Forgery.This issue affects Table of Contents Plus: from n/a through 2408.	2024-10-20	4.3	CVE-2024-49250
Microchip--RN4870	On Microchip RN4870 devices, when more than one consecutive PairReqNoInputNoOutput request is received, the device becomes incapable of completing the pairing process. A third party can inject a second PairReqNoInputNoOutput request just after a real one, causing the pair request to be blocked.	2024-10-16	4.3	CVE-2024-29155
microsoft -- edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-10-17	5.4	CVE-2024-43580
microsoft -- edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-10-18	5.3	CVE-2024-49023

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-10-18	4.3	CVE-2024-43577
Mighty Plugins--Mighty Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mighty Plugins Mighty Builder allows Stored XSS.This issue affects Mighty Builder: from n/a through 1.0.2.	2024-10-20	6.5	CVE-2024-48049
mikexstudios--Xcomic	A vulnerability classified as critical has been found in mikexstudios Xcomic up to 0.8.2. This affects an unknown part. The manipulation of the argument cmd leads to os command injection. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 0.8.3 is able to address this issue. The patch is named 6ed8e3cc336e29f09c7e791863d0559939da98bf. It is recommended to upgrade the affected component.	2024-10-17	5.6	CVE-2005-10003
MitraStar--GPT-2541GNAC	A vulnerability, which was classified as critical, was found in MitraStar GPT-2541GNAC BR_g5.6_1.11(WVK.0)b26. Affected is an unknown function of the file /cgi-bin/settings-firewall.cgi of the component Firewall Settings Page. The manipulation of the argument SrcInterface leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	2024-10-15	4.7	CVE-2024-9977
Mitsubishi Electric Corporation--Mitsubishi Electric CNC M800V Series M800VW	Improper Validation of Specified Quantity in Input vulnerability in Mitsubishi Electric CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition on the product by sending specially crafted packets to TCP port 683, causing an emergency stop.	2024-10-17	5.9	CVE-2024-7316
morceaudebois--Debrandify Remove or Replace WordPress Branding	The Debrandify Â· Remove or Replace WordPress Branding plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-18	6.4	CVE-2024-9674
Moxa--MXsecurity Series	The lack of access restriction to a resource from unauthorized users makes MXsecurity software versions v1.1.0 and prior vulnerable. By acquiring a valid authenticator, an attacker can pose as an authorized user and successfully access the resource.	2024-10-18	5.3	CVE-2024-4739
n/a--CoinGate Plugin	A vulnerability was found in CoinGate Plugin up to 1.2.7 on PrestaShop. It has been rated as problematic. Affected by this issue is the function postProcess of the file modules/coingate/controllers/front/callback.php of the component Payment Handler. The manipulation leads to business logic errors. The attack may be launched remotely. Upgrading to version 1.2.8 is able to address this issue. The patch is identified as 0a3097db0aec7c5d66686c142c6abaa1e126ca16. It is recommended to upgrade the affected component.	2024-10-17	4.3	CVE-2018-25104
n/a--n/a	RCE (Remote Code Execution) exists in ZoneMinder through 1.36.33 as an attacker can create a new .php log file in language folder, while executing a crafted payload and escalate privileges allowing execution of any commands on the remote system.	2024-10-15	6.6	CVE-2023-31493

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	An issue was discovered in version of Warp Terminal prior to 2024.07.18 (v0.2024.07.16.08.02). A command injection vulnerability exists in the Docker integration functionality. An attacker can create a specially crafted hyperlink using the `warp://action/docker/open_subshell` intent that when clicked by the victim results in command execution on the victim's machine.	2024-10-14	6.6	CVE-2024-41997
n/a--n/a	An Insecure Direct Object Reference (IDOR) vulnerability in KubeSphere v3.4.1 and v4.1.1 allows low-privileged authenticated attackers to access sensitive resources without proper authorization checks.	2024-10-14	6.5	CVE-2024-46528
n/a--n/a	A cross-site scripting (XSS) vulnerability in the component /admin.php?page=album of Piwigo v14.5.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Description field.	2024-10-16	6.1	CVE-2024-46605
n/a--n/a	X2CRM v8.5 is vulnerable to a stored Cross-Site Scripting (XSS) in the "Opportunities" module. An attacker can inject malicious JavaScript code into the "Name" field when creating a list.	2024-10-14	6.5	CVE-2024-48120
n/a--n/a	A cross-site scripting (XSS) issue in DomainMOD below v4.12.0 allows remote attackers to inject JavaScript code via admin/domain-fields/edit.php and the cdfid parameter.	2024-10-15	6.6	CVE-2024-48622
n/a--n/a	In TP-Link TL-WDR7660 1.0, the wlanTimerRuleJsonToBin function handles the parameter string name without checking it, which can lead to stack overflow vulnerabilities.	2024-10-15	6.5	CVE-2024-48710
n/a--n/a	In TP-Link TL-WDR7660 1.0, the rtRuleJsonToBin function handles the parameter string name without checking it, which can lead to stack overflow vulnerabilities.	2024-10-15	6.5	CVE-2024-48712
n/a--n/a	In TP-Link TL-WDR7660 1.0, the wacWhitelistJsonToBin function handles the parameter string name without checking it, which can lead to stack overflow vulnerabilities.	2024-10-15	6.5	CVE-2024-48713
n/a--n/a	In TP-Link TL-WDR7660 v1.0, the guestRuleJsonToBin function handles the parameter string name without checking it, which can lead to stack overflow vulnerabilities.	2024-10-15	6.5	CVE-2024-48714
n/a--n/a	A Reflected Cross Site Scripting (XSS) vulnerability was found in /trms/listed-teachers.php in PHPGurukul Teachers Record Management System v2.1, which allows remote attackers to execute arbitrary code via "searchinput" POST request parameter.	2024-10-16	6.1	CVE-2024-48744
n/a--n/a	dingfanzu CMS V1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the addPro parameter of the component doAdminAction.php which allows a remote attacker to execute arbitrary code	2024-10-16	6.1	CVE-2024-48758
n/a--n/a	Cross Site Scripting vulnerability in Automatic Systems Maintenance SlimLane 29565_d74ecce0c1081d50546db573a499941b10799fb7 allows a remote attacker to escalate privileges via the FtpConfig.php component.	2024-10-14	6.1	CVE-2024-48821
n/a--n/a	Insecure permissions in the sys_exec function of MariaDB v10.5 allows authenticated attackers to execute arbitrary commands with elevated privileges. NOTE: this is disputed by the MariaDB Foundation because no privilege boundary is crossed.	2024-10-17	5.6	CVE-2023-39593
n/a--n/a	An issue in MariaDB v.11.1 allows a remote attacker to execute arbitrary code via the lib_mysqludf_sys.so function. NOTE: this is disputed by the MariaDB Foundation because no privilege boundary is crossed.	2024-10-17	5.7	CVE-2024-27766

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	A discrepancy in error messages for invalid login attempts in Webmin Usermin v2.100 allows attackers to enumerate valid user accounts.	2024-10-16	5.3	CVE-2024-44762
n/a--n/a	A cross-site scripting (XSS) vulnerability in the component /admin.php?page=photo of Piwigo v14.5.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Description field.	2024-10-16	5.4	CVE-2024-46606
n/a--n/a	Vtiger CRM v8.2.0 has a HTML Injection vulnerability in the module parameter. Authenticated users can inject arbitrary HTML.	2024-10-14	5.4	CVE-2024-48119
n/a--n/a	Phpgurukul User Registration & Login and User Management System 3.2 is vulnerable to Cross Site Request Forgery (CSRF) via /edit-profile.php.	2024-10-15	5.5	CVE-2024-48278
n/a--n/a	In queue\index.php of DomainMOD below v4.12.0, the list_id and domain_id parameters in the GET request can be exploited to cause a reflected Cross Site Scripting (XSS).	2024-10-15	5.3	CVE-2024-48623
n/a--n/a	In segments\edit.php of DomainMOD below v4.12.0, the segid parameter in the GET request can be exploited to cause a reflected Cross Site Scripting (XSS) vulnerability.	2024-10-15	5.3	CVE-2024-48624
n/a--n/a	An issue in ILIFE com.ilife.home.global 1.8.7 allows a remote attacker to obtain sensitive information via the firmware update process.	2024-10-14	5.3	CVE-2024-48790
n/a--n/a	An issue in INATRONIC com.inatronic.bmw 2.7.1 allows a remote attacker to obtain sensitive information via the firmware update process.	2024-10-14	5.9	CVE-2024-48793
n/a--n/a	An issue in Creative Labs Pte Ltd com.creative.apps.xficonnect 2.00.02 allows a remote attacker to obtain sensitive information via the firmware update process.	2024-10-14	5.3	CVE-2024-48795
n/a--n/a	QUIC in HAProxy 3.1.x before 3.1-dev7, 3.0.x before 3.0.5, and 2.9.x before 2.9.11 allows opening a 0-RTT session with a spoofed IP address. This can bypass the IP allow/block list functionality.	2024-10-14	5.3	CVE-2024-49214
n/a--n/a	An issue was discovered in Samsung eMMC with KLMAG2GE4A and KLM8G1WEMB firmware. Code bypass through Electromagnetic Fault Injection allows an attacker to successfully authenticate and write to the RPMB (Replay Protected Memory Block) area without possessing secret information.	2024-10-15	4.9	CVE-2024-31955
n/a--n/a	An issue in the component /index.php?page=backup/export of REDAXO CMS v5.17.1 allows attackers to execute a directory traversal.	2024-10-16	4.9	CVE-2024-46212
nayon46--Unlimited Addon For Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in nayon46 Unlimited Addon For Elementor allows Stored XSS.This issue affects Unlimited Addon For Elementor: from n/a through 2.0.0.	2024-10-16	6.5	CVE-2024-49267
netgear --ex3700_firmware	Netgear EX6120 v1.0.0.68, Netgear EX6100 v1.0.2.28, and Netgear EX3700 v1.0.0.96 are vulnerable to command injection in operating_mode.cgi via the ap_mode parameter.	2024-10-14	6.8	CVE-2024-35519
netgear --ex6120_firmware	Netgear EX6120 v1.0.0.68 is vulnerable to Command Injection in genie_fix2.cgi via the wan_dns1_pri parameter.	2024-10-14	6.8	CVE-2024-35518
netgear --r7000_firmware	Netgear R7000 1.0.11.136 is vulnerable to Command Injection in RMT_invite.cgi via device_name2 parameter.	2024-10-14	6.8	CVE-2024-35520

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
newtype -- webeip	NewType WebEIP v3.0 does not properly validate user input, allowing a remote attacker with regular privileges to insert JavaScript into specific parameters, resulting in a Reflected Cross-site Scripting (XSS) attack. The affected product is no longer maintained. It is recommended to upgrade to the new product.	2024-10-15	5.4	CVE-2024-9969
nextscripts--NextScripts: Social Networks Auto-Poster	The NextScripts: Social Networks Auto-Poster plugin for WordPress is vulnerable to authorization bypass due to missing capability checks on multiple user privilege/security functions provided in versions up to, and including 4.3.17. This makes it possible for low-privileged attackers, like subscribers, to perform restricted actions that would be otherwise locked to a administrative-level user.	2024-10-16	5	CVE-2020-36831
NicheAddons--Events Addon for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Events Addon for Elementor allows Stored XSS.This issue affects Events Addon for Elementor: from n/a through 2.2.0.	2024-10-17	6.5	CVE-2024-49264
NicheAddons--Primary Addon for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Primary Addon for Elementor allows Stored XSS.This issue affects Primary Addon for Elementor: from n/a through 1.5.8.	2024-10-17	6.5	CVE-2024-49259
nik00726--Photo Gallery Slideshow & Masonry Tiled Gallery	The Photo Gallery Slideshow & Masonry Tiled Gallery plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 1.0.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-10-19	4.9	CVE-2019-25218
nik00726--Video Grid	The Video Grid plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.21 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-16	6.1	CVE-2023-7295
NinjaTeam--Click to Chat WP Support All-in-One Floating Widget	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NinjaTeam Click to Chat - WP Support All-in-One Floating Widget allows Stored XSS.This issue affects Click to Chat - WP Support All-in-One Floating Widget: from n/a through 2.3.3.	2024-10-17	6.5	CVE-2024-49281
ninjateam--Click to Chat WP Support All-in-One Floating Widget	The Click to Chat - WP Support All-in-One Floating Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpsaio_snapchat shortcode in all versions up to, and including, 2.3.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-18	6.4	CVE-2024-10055
nintechnet--NinjaFirewall (WP Edition) Advanced Security Plugin and Firewall	The NinjaFirewall plugin for WordPress is vulnerable to Authenticated PHAR Deserialization in versions up to, and including, 4.3.3. This allows authenticated attackers to perform phar deserialization on the server. This deserialization can allow other plugin or theme exploits if vulnerable software is present (WordPress, and NinjaFirewall).	2024-10-16	6.6	CVE-2021-4451

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Noor Alam--WordPress Image SEO	Cross-Site Request Forgery (CSRF) vulnerability in Noor Alam WordPress Image SEO allows Cross Site Request Forgery.This issue affects WordPress Image SEO: from n/a through 1.1.4.	2024-10-20	4.3	CVE-2024-49627
NVIDIA--NeMo	NVIDIA NeMo contains a vulnerability in SaveRestoreConnector where a user may cause a path traversal issue via an unsafe .tar file extraction. A successful exploit of this vulnerability may lead to code execution and data tampering.	2024-10-15	6.3	CVE-2024-0129
OISF--suricata	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Prior to version 7.0.7, a logic error during fragment reassembly can lead to failed reassembly for valid traffic. An attacker could craft packets to trigger this behavior.This issue has been addressed in 7.0.7.	2024-10-16	5.3	CVE-2024-45796
Oliver Schlbe--Admin Management Xtended	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Oliver SchlÃ¶be Admin Management Xtended allows Stored XSS.This issue affects Admin Management Xtended: from n/a through 2.4.6.	2024-10-17	6.5	CVE-2024-49307
omnipressteam--Omnipress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in omnipressteam Omnipress allows Stored XSS.This issue affects Omnipress: from n/a through 1.4.3.	2024-10-17	6.5	CVE-2024-49278
opajaap--WP Photo Album Plus	The WP Photo Album Plus plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'wppa-tab' parameter in all versions up to, and including, 8.8.05.003 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-17	6.1	CVE-2024-9951
oracle -- fusion_middleware	Vulnerability in the Oracle Service Bus product of Oracle Fusion Middleware (component: OSB Core Functionality). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Service Bus. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Service Bus accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2024-10-15	6.5	CVE-2024-21205
oracle -- fusion_middleware	Vulnerability in the Oracle Enterprise Manager for Fusion Middleware product of Oracle Fusion Middleware (component: WebLogic Mgmt). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Enterprise Manager for Fusion Middleware executes to compromise Oracle Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Manager for Fusion Middleware accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2024-10-15	4.4	CVE-2024-21192
oracle -- graalvm	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to	2024-10-15	4.8	CVE-2024-21235

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: X Plugin). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	6.5	CVE-2024-21196
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	6.5	CVE-2024-21230
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.39 and prior, 8.4.1 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	5.3	CVE-2024-21238
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21193
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21194
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	2024-10-15	4.9	CVE-2024-21197

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21198
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21199
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21200
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21201
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21203
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.4.0 and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21204

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.38 and prior, 8.4.1 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21207
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Health Monitor). Supported versions that are affected are 8.0.39 and prior and 8.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.4	CVE-2024-21212
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H).	2024-10-15	4.2	CVE-2024-21213
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21218
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21219
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21236
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	2024-10-15	4.9	CVE-2024-21239

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-10-15	4.9	CVE-2024-21241
oracle -- peoplesoft_enterprise_people_tools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2024-10-15	6.1	CVE-2024-21202
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H).	2024-10-15	6.1	CVE-2024-21263
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2024-10-15	6	CVE-2024-21273
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data and unauthorized ability to	2024-10-15	5.3	CVE-2024-21248

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L).			
Oracle Corporation--MySQL Connectors	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/ODBC). Supported versions that are affected are 9.0.0 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	2024-10-15	6.5	CVE-2024-21262
Oracle Corporation--Oracle Application Express	Vulnerability in Oracle Application Express (component: General). Supported versions that are affected are 23.2 and 24.1. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Express. While the vulnerability is in Oracle Application Express, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express accessible data as well as unauthorized read access to a subset of Oracle Application Express accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N).	2024-10-15	4.9	CVE-2024-21261
Oracle Corporation--Oracle Banking Liquidity Management	Vulnerability in the Oracle Banking Liquidity Management product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.7.0.6.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Liquidity Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Liquidity Management accessible data as well as unauthorized read access to a subset of Oracle Banking Liquidity Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Liquidity Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:H/A:L).	2024-10-15	5.3	CVE-2024-21281
Oracle Corporation--Oracle Database Server	Vulnerability in the Oracle Database Core component of Oracle Database Server. Supported versions that are affected are 19.3-19.24, 21.3-21.15 and 23.4-23.5. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database Core. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database Core accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2024-10-15	4.3	CVE-2024-21233
Oracle Corporation--Oracle Enterprise Command Center Framework	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are ECC:11-13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2024-10-15	4.3	CVE-2024-21206
Oracle Corporation--	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.2.3-	2024-10-15	5.3	CVE-2024-21258

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Installed Base	12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Installed Base accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
Oracle Corporation--PeopleSoft Enterprise CC Common Application Objects	Vulnerability in the PeopleSoft Enterprise CC Common Application Objects product of Oracle PeopleSoft (component: Activity Guide Composer). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CC Common Application Objects. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise CC Common Application Objects accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise CC Common Application Objects accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2024-10-15	5.4	CVE-2024-21264
Oracle Corporation--PeopleSoft Enterprise ELM Enterprise Learning Management	Vulnerability in the PeopleSoft Enterprise ELM Enterprise Learning Management product of Oracle PeopleSoft (component: Enterprise Learning Management). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise ELM Enterprise Learning Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise ELM Enterprise Learning Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2024-10-15	5.4	CVE-2024-21286
Oracle Corporation--PeopleSoft Enterprise FIN Expenses	Vulnerability in the PeopleSoft Enterprise FIN Expenses product of Oracle PeopleSoft (component: Expenses). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Expenses. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise FIN Expenses accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2024-10-15	4.3	CVE-2024-21249
oretnom23 -- online_eyewear_shop	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/?page=system_info/contact_info of the component Contact Information Page. The manipulation of the argument Address leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2024-10-15	4.8	CVE-2024-9952
parcelpro--Parcel Pro	The Parcel Pro plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'action' parameter in all versions up to, and including, 1.8.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-18	6.1	CVE-2024-9383
paretodigital--YASR Yet Another Star Rating Plugin for WordPress	The Freemius SDK, as used by hundreds of WordPress plugin and theme developers, was vulnerable to Cross-Site Request Forgery and Information disclosure due to missing capability checks and nonce protection on the _get_debug_log, _get_db_option, and the _set_db_option functions in versions up	2024-10-16	6.3	CVE-2022-4974

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to, and including 2.4.2. Any WordPress plugin or theme running a version of Freemius less than 2.4.3 is vulnerable.			
Partnerships at Booking.com--Booking.com Banner Creator	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Partnerships at Booking.Com Booking.Com Banner Creator allows Stored XSS.This issue affects Booking.Com Banner Creator: from n/a through 1.4.6.	2024-10-16	6.5	CVE-2024-49265
paulirish-1--Infinite-Scroll	The Infinite-Scroll plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.2. This is due to missing or incorrect nonce validation on the process_ajax_edit and process_ajax_delete function. This makes it possible for unauthenticated attackers to make changes to plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-10-18	5.3	CVE-2024-10040
paytium -- paytium	The Paytium: Mollie payment forms & donations plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the create_mollie_profile function in versions up to, and including, 4.3.7. This makes it possible for authenticated attackers with subscriber-level access to create a mollie payment profile.	2024-10-16	6.5	CVE-2023-7294
paytium -- paytium	The Paytium: Mollie payment forms & donations plugin for WordPress is vulnerable to unauthorized subscription cancellation due to a missing capability check on the pt_cancel_subscription function in versions up to, and including, 4.3.7. This makes it possible for authenticated attackers with subscriber-level access to cancel a subscription to the plugin.	2024-10-16	5.4	CVE-2023-7287
paytium -- paytium	The Paytium: Mollie payment forms & donations plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the update_profile_preference function in versions up to, and including, 4.3.7. This makes it possible for authenticated attackers with subscriber-level access to change plugin settings.	2024-10-16	4.3	CVE-2023-7288
paytium -- paytium	The Paytium: Mollie payment forms & donations plugin for WordPress is vulnerable to unauthorized API key update due to a missing capability check on the paytium_sw_save_api_keys function in versions up to, and including, 4.3.7. This makes it possible for authenticated attackers with subscriber-level access to change plugin API keys.	2024-10-16	4.3	CVE-2023-7289
paytium -- paytium	The Paytium: Mollie payment forms & donations plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the check_for_verified_profiles function in versions up to, and including, 4.3.7. This makes it possible for authenticated attackers with subscriber-level access to check profile statuses.	2024-10-16	4.3	CVE-2023-7290
paytium -- paytium	The Paytium: Mollie payment forms & donations plugin for WordPress is vulnerable to unauthorized notification dismissal due to a missing capability check on the paytium_notice_dismiss function in versions up to, and including, 4.3.7. This makes it possible for authenticated attackers with subscriber-level access to dismiss admin notices.	2024-10-16	4.3	CVE-2023-7292
paytium -- paytium	The Paytium: Mollie payment forms & donations plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the check_mollie_account_details function in versions up to, and including, 4.3.7. This makes it possible for authenticated attackers with subscriber-level access to verify the existence of a mollie account.	2024-10-16	4.3	CVE-2023-7293
peepso--Community by	The Community by PeepSo - Social Network, Membership, Registration, User Profiles, Premium - Mobile App plugin for WordPress is vulnerable to Stored Cross-	2024-10-16	5.4	CVE-2024-9873

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
PeepSo Social Network, Membership, Registration, User Profiles, Premium Mobile App	Site Scripting via URLs in posts, comments, and profiles when Markdown support is enabled in all versions up to, and including, 6.4.6.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
Pepro Dev. Group--PeproDev Ultimate Invoice	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pepro Dev. Group PeproDev Ultimate Invoice allows Stored XSS.This issue affects PeproDev Ultimate Invoice: from n/a through 2.0.6.	2024-10-17	6.5	CVE-2024-49298
persianscript--Persian WooCommerce SMS	The ?????? ????? ??????? Persian WooCommerce SMS plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 7.0.2. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-17	6.1	CVE-2024-9213
Peter CyClop--WordPress Video	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Peter CyClop WordPress Video allows Stored XSS.This issue affects WordPress Video: from n/a through 1.0.	2024-10-18	6.5	CVE-2024-49231
PHPGurukul--Boat Booking System	A vulnerability has been found in PHPGurukul Boat Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file book-boat.php?bid=1 of the component Book a Boat Page. The manipulation of the argument nopeople leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-19	6.3	CVE-2024-10153
PHPGurukul--Boat Booking System	A vulnerability was found in PHPGurukul Boat Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file status.php of the component Check Booking Status Page. The manipulation of the argument emailid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-19	6.3	CVE-2024-10154
PHPGurukul--Boat Booking System	A vulnerability, which was classified as critical, has been found in PHPGurukul Boat Booking System 1.0. Affected by this issue is some unknown functionality of the file /admin/bwdates-report-details.php of the component BW Dates Report Page. The manipulation of the argument fdate/tdate leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "fdate" to be affected. But it must be assumed "tdate" is affected as well.	2024-10-20	6.3	CVE-2024-10160
PHPGurukul--Boat Booking System	A vulnerability, which was classified as critical, was found in PHPGurukul Boat Booking System 1.0. This affects an unknown part of the file change-image.php of the component Update Boat Image Page. The manipulation of the argument image leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-20	6.3	CVE-2024-10161
PHPGurukul--Boat Booking System	A vulnerability has been found in PHPGurukul Boat Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/edit-subadmin.php of the component Edit Subdomain Details Page. The manipulation of the argument sadminusername/fullname/emailid/mobilenumber leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "mobilenumber" to be affected. But it must be assumed that other parameters are affected as well.	2024-10-20	6.3	CVE-2024-10162

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
PHPGurukul--Boat Booking System	A vulnerability classified as problematic has been found in PHPGurukul Boat Booking System 1.0. Affected is the function session_start. The manipulation leads to session fixiation. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-19	4.3	CVE-2024-10158
PINPOINT.WORLD --Pinpoint Booking System	Cross-Site Request Forgery (CSRF) vulnerability in PINPOINT.WORLD Pinpoint Booking System allows Stored XSS.This issue affects Pinpoint Booking System: from n/a through 2.9.9.5.1.	2024-10-17	5.4	CVE-2024-49304
plainware--Locatoraid Store Locator	The Locatoraid Store Locator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via $_POST keys in all versions up to, and including, 3.9.47 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-16	6.1	CVE-2024-9652
podpirate--ACF Quick Edit Fields	The plugin ACF Quick Edit Fields for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 3.2.2. This makes it possible for attackers without the edit_users capability to access metadata of other users, this includes contributor-level users and above.	2024-10-16	6.5	CVE-2023-7286
Portfoliohub--WordPress Portfolio Builder Portfolio Gallery	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Portfoliohub WordPress Portfolio Builder - Portfolio Gallery allows Stored XSS.This issue affects WordPress Portfolio Builder - Portfolio Gallery: from n/a through 1.1.7.	2024-10-17	6.5	CVE-2024-49302
prasidhda--Woo Manage Fraud Orders	The Woo Manage Fraud Orders plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 6.1.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-16	6.1	CVE-2024-9937
PressTigers--Simple Testimonials Showcase	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PressTigers Simple Testimonials Showcase.This issue affects Simple Testimonials Showcase: from n/a through 1.1.6.	2024-10-17	5.9	CVE-2024-49295
quantizor --markdown-to-jsx	Versions of the package markdown-to-jsx before 7.4.0 are vulnerable to Cross-site Scripting (XSS) via the src property due to improper input sanitization. An attacker can execute arbitrary code by injecting a malicious iframe element in the markdown.	2024-10-15	6.1	CVE-2024-21535
quomodosoft--ElementsReady Addons for Elementor	The ElementsReady Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 6.4.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-16	6.4	CVE-2024-9444
Razon Komar Pal--Linked Variation for WooCommerce	Cross-Site Request Forgery (CSRF) vulnerability in Razon Komar Pal Linked Variation for WooCommerce allows Cross Site Request Forgery.This issue affects Linked Variation for WooCommerce: from n/a through 1.0.5.	2024-10-17	4.3	CVE-2024-48047

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--OpenShift Developer Tools and Services	A vulnerability was found in Podman, Buildah, and CRI-O. A symlink traversal vulnerability in the containers/storage library can cause Podman, Buildah, and CRI-O to hang and result in a denial of service via OOM kill when running a malicious image using an automatically assigned user namespace (`--userns=auto` in Podman and Buildah). The containers/storage library will read /etc/passwd inside the container, but does not properly validate if that file is a symlink, which can be used to cause the library to read an arbitrary file on the host.	2024-10-15	6.5	CVE-2024-9676
Red Hat--Red Hat Ansible Automation Platform 2	A vulnerability was found in aap-gateway. A Cross-site Scripting (XSS) vulnerability exists in the gateway component. This flaw allows a malicious user to perform actions that impact users by using the "?next=" in a URL, which can lead to redirecting, injecting malicious script, stealing sessions and data.	2024-10-16	5.4	CVE-2024-10033
Red Hat--Red Hat Ansible Automation Platform 2	A flaw was found in PyO3. This vulnerability causes a use-after-free issue, potentially leading to memory corruption or crashes via unsound borrowing from weak Python references.	2024-10-15	5.3	CVE-2024-9979
Red Hat--Red Hat Quay 3	A vulnerability was found in Quay, which allows successful authentication even when a truncated password version is provided. This flaw affects the authentication mechanism, reducing the overall security of password enforcement. While the risk is relatively low due to the typical length of the passwords used (73 characters), this vulnerability can still be exploited to reduce the complexity of brute-force or password-guessing attacks. The truncation of passwords weakens the overall authentication process, thereby reducing the effectiveness of password policies and potentially increasing the risk of unauthorized access in the future.	2024-10-17	4.8	CVE-2024-9683
RITTAL GmbH & Co. KG--IoT Interface & CMC III Processing Unit	The device directly executes .patch firmware upgrade files on a USB stick without any prior authentication in the admin interface. This leads to an unauthenticated code execution via the firmware upgrade function.	2024-10-15	6.8	CVE-2024-47944
sajjad67--Advanced Category and Custom Taxonomy Image	The Advanced Category and Custom Taxonomy Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ad_tax_image shortcode in all versions up to, and including, 1.0.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-18	6.4	CVE-2024-9425
shaonsina--Sina Extension for Elementor (Slider, Gallery, Form, Modal, Data Table, Tab, Particle, Free Elementor Widgets & Elementor Templates)	The Sina Extension for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.5.7 via the render function in widgets/advanced/sina-modal-box.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft Elementor template data.	2024-10-16	4.3	CVE-2024-9540

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Sinan Yorulmaz--G Meta Keywords	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sinan Yorulmaz G Meta Keywords allows Stored XSS.This issue affects G Meta Keywords: from n/a through 1.4.	2024-10-17	6.5	CVE-2024-49301
SKT Themes--SKT Blocks Gutenberg based Page Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SKT Themes SKT Blocks - Gutenberg based Page Builder allows Stored XSS.This issue affects SKT Blocks - Gutenberg based Page Builder: from n/a through 1.6.	2024-10-17	6.5	CVE-2024-48036
smackcoders--SendGrid for WordPress	The SendGrid for WordPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'wp_mailplus_clear_logs' function in all versions up to, and including, 1.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete the plugin's log files.	2024-10-18	4.3	CVE-2024-9364
SolarWinds--Kiwi CatTools	SolarWinds Kiwi CatTools is susceptible to a sensitive data disclosure vulnerability when a non-default setting has been enabled for troubleshooting purposes.	2024-10-17	5.1	CVE-2024-45713
SolarWinds--Serv-U	Application is vulnerable to Cross Site Scripting (XSS) an authenticated attacker with users' permissions can modify a variable with a payload.	2024-10-16	4.8	CVE-2024-45714
SourceCodester--Sentiment Based Movie Rating System	A vulnerability was found in SourceCodester Sentiment Based Movie Rating System 1.0. It has been classified as critical. Affected is an unknown function of the file /msrps/movie_details.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher disclosure mentions a slightly changed product name.	2024-10-20	6.3	CVE-2024-10163
splunk -- splunk	In Splunk Enterprise versions below 9.3.1, and 9.2.0 versions below 9.2.3, and Splunk Cloud Platform versions below 9.2.2403.103, 9.1.2312.200, 9.1.2312.110 and 9.1.2308.208, a low-privileged user that does not hold the "admin" or "power" Splunk roles could run a search as the "nobody" Splunk user in the SplunkDeploymentServerConfig app. This could let the low-privileged user access potentially restricted data.	2024-10-14	6.5	CVE-2024-45732
splunk -- splunk	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403.107, 9.1.2312.204, and 9.1.2312.111, a low-privileged user that does not hold the "admin" or "power" Splunk roles could craft a search query with an improperly formatted "INGEST_EVAL" parameter as part of a [Field Transformation](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Managefieldtransforms) which could crash the Splunk daemon (splunkd).	2024-10-14	6.5	CVE-2024-45736
splunk -- splunk	In Splunk Enterprise versions below 9.2.3 and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403, a low-privileged user that does not hold the "admin" or "power" Splunk roles could craft a malicious payload through Scheduled Views that could result in execution of unauthorized JavaScript code in the browser of a user.	2024-10-14	5.4	CVE-2024-45740
splunk -- splunk	In Splunk Enterprise versions below 9.2.3 and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403.108 and 9.1.2312.205, a low-privileged user that does not hold the "admin" or "power" Splunk roles could create a malicious payload through a custom configuration file that the "api.uri" parameter from the "/manager/search/apps/local" endpoint in Splunk Web calls. This could result in execution of unauthorized JavaScript code in the browser of a user.	2024-10-14	5.4	CVE-2024-45741

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
splunk -- splunk	In Splunk Enterprise versions 9.3.0, 9.2.3, and 9.1.6, a low-privileged user that does not hold the "admin" or "power" Splunk roles could view images on the machine that runs Splunk Enterprise by using the PDF export feature in Splunk classic dashboards. The images on the machine could be exposed by exporting the dashboard as a PDF, using the local image path in the img tag in the source extensible markup language (XML) code for the Splunk classic dashboard.	2024-10-14	4.3	CVE-2024-45734
splunk -- splunk	In Splunk Enterprise versions below 9.2.3 and 9.1.6, and Splunk Secure Gateway versions on Splunk Cloud Platform versions below 3.4.259, 3.6.17, and 3.7.0, a low-privileged user that does not hold the "admin" or "power" Splunk roles can see App Key Value Store (KV Store) deployment configuration and public/private keys in the Splunk Secure Gateway App.	2024-10-14	4.3	CVE-2024-45735
splunk -- splunk	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6, the software potentially exposes sensitive HTTP parameters to the `_internal` index. This exposure could happen if you configure the Splunk Enterprise `REST_Calls` log channel at the DEBUG logging level.	2024-10-14	4.9	CVE-2024-45738
splunk -- splunk	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6, the software potentially exposes plaintext passwords for local native authentication Splunk users. This exposure could happen when you configure the Splunk Enterprise AdminManager log channel at the DEBUG logging level.	2024-10-14	4.9	CVE-2024-45739
strategy11team--Formidable Forms Contact Form Plugin, Survey, Quiz, Payment, Calculator Form & Custom Form Builder	The Formidable Form Builder plugin for WordPress is vulnerable to Sensitive Data Exposure in versions up to, and including, 2.05.03 via the frm_forms_preview AJAX action. This makes it possible for unauthenticated attackers to export all of the form entries for a given form.	2024-10-16	5.3	CVE-2017-20194
Streamline.lv--CartBounty Save and recover abandoned carts for WooCommerce	Cross-Site Request Forgery (CSRF) vulnerability in Streamline.Lv CartBounty - Save and recover abandoned carts for WooCommerce allows Cross Site Request Forgery.This issue affects CartBounty - Save and recover abandoned carts for WooCommerce: from n/a through 8.2.	2024-10-20	6.5	CVE-2024-47634
streamweasels--StreamWeasels Twitch Integration	The StreamWeasels Twitch Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's sw-twitch-embed shortcode in all versions up to, and including, 1.8.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-19	6.4	CVE-2024-9897
sukiwp--Suki Sites Import	The Suki Sites Import plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-18	6.4	CVE-2024-8916
Sumit Surai--Featured Posts with Multiple Custom Groups	Cross-Site Request Forgery (CSRF) vulnerability in Sumit Surai Featured Posts with Multiple Custom Groups (FPMCG) allows Cross Site Request Forgery.This issue affects Featured Posts with Multiple Custom Groups (FPMCG): from n/a through 4.0.	2024-10-17	6.5	CVE-2024-48031

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
(FPMCG)				
Supsystic--Contact Form by Supsystic	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Supsystic Contact Form by Supsystic allows Stored XSS.This issue affects Contact Form by Supsystic: from n/a through 1.7.28.	2024-10-17	5.9	CVE-2024-48046
SUSE--rancher	A vulnerability has been identified whereby privilege escalation checks are not properly enforced for RoleTemplateobjects when external=true, which in specific scenarios can lead to privilege escalation.	2024-10-16	6.6	CVE-2023-32196
SUSE--rancher	A vulnerability has been identified in which an RKE1 cluster keeps constantly reconciling when secrets encryption configuration is enabled. When reconciling, the Kube API secret values are written in plaintext on the AppliedSpec. Cluster owners, Cluster members, and Project members (for projects within the cluster), all have RBAC permissions to view the cluster object from the apiserver.	2024-10-16	6.5	CVE-2024-22032
SUSE--SUSE Linux Enterprise Desktop 15 SP5	Attackers could put the special files in .osc into the actual package sources (e.g. _apiurl). This allows the attacker to change the configuration of osc for the victim	2024-10-16	5.5	CVE-2024-22034
SUSE--SUSE Manager Server Module 4.3	Insecure handling of ssh keys used to bootstrap clients allows local attackers to potentially gain access to the keys	2024-10-16	5.9	CVE-2023-32189
SUSE--SUSE Package Hub 15 SP5	The OBS service obs-service-download_url was vulnerable to a command injection vulnerability. The attacker could provide a configuration to the service that allowed to execute command in later steps	2024-10-16	6.3	CVE-2024-22033
Swebdeveloper--wpPricing Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Swebdeveloper wpPricing Builder allows Stored XSS.This issue affects wpPricing Builder: from n/a through 1.5.0.	2024-10-18	6.5	CVE-2024-49225
SysBasics--Shortcode For Elementor Templates	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SysBasics Shortcode For Elementor Templates allows Stored XSS.This issue affects Shortcode For Elementor Templates: from n/a through 1.0.0.	2024-10-17	6.5	CVE-2024-48022
Tady Walsh--Tito	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tady Walsh Tito allows DOM-Based XSS.This issue affects Tito: from n/a through 2.3.	2024-10-18	6.5	CVE-2024-49241
Takashi Matsuyama--My Favorites	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Takashi Matsuyama My Favorites allows Stored XSS.This issue affects My Favorites: from n/a through 1.4.1.	2024-10-17	6.5	CVE-2024-49263
teamplus technology--team+	The Team+ from TEAMPLUS TECHNOLOGY does not properly validate a specific page parameter, allowing remote attackers with administrator privileges to move arbitrary system files to the website root directory and access them.	2024-10-14	4.9	CVE-2024-9923
Tecno--4G Portable WiFi	A vulnerability was found in Tecno 4G Portable WiFi TR118 V008-20220830. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /goform/goform_get_cmd_process of the component SMS Check. The manipulation of the argument order_by leads to sql injection. The attack can be	2024-10-20	4.7	CVE-2024-10195

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
TR118	launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.			
Teplitsa of social technologies--Leyka	: Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Teplitsa of social technologies Leyka.This issue affects Leyka: from n/a through 3.31.6.	2024-10-16	5.3	CVE-2024-49252
thecatkin--ReDi Restaurant Reservation	The ReDi Restaurant Reservation plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 24.0902. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-17	6.1	CVE-2024-9240
thehowarde--Parallax Image	The Parallax Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's dd-parallax shortcode in all versions up to, and including, 1.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-17	6.4	CVE-2024-9898
themeid--Elemenda	The Elemenda plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 0.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-18	6.4	CVE-2024-9373
themeinwp--Social Share With Floating Bar	The Social Share With Floating Bar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.0.3. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-18	6.1	CVE-2024-8790
Themesflat--Themesflat Addons For Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themesflat Themesflat Addons For Elementor allows Stored XSS.This issue affects Themesflat Addons For Elementor: from n/a through 2.2.0.	2024-10-17	6.5	CVE-2024-49310
themeworm--Plexx Elementor Extension	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in themeworm Plexx Elementor Extension allows Stored XSS.This issue affects Plexx Elementor Extension: from n/a through 1.3.4.	2024-10-18	6.5	CVE-2024-49234
Thimo Grauerholz--WP-Spreadplugin	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Thimo Grauerholz WP-Spreadplugin allows Stored XSS.This issue affects WP-Spreadplugin: from n/a through 4.8.9.	2024-10-16	5.9	CVE-2024-49266
tiandi--Flat UI Button	The Flat UI Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's flatbtn shortcode in version 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-18	6.4	CVE-2024-10014

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
TipTopPress--Hyperlink Group Block	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TipTopPress Hyperlink Group Block allows Stored XSS.This issue affects Hyperlink Group Block: from n/a through 1.17.5.	2024-10-17	6.5	CVE-2024-49279
tkama--Kama SpamBlock	The Kama SpamBlock plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via $_POST values in all versions up to, and including, 1.8.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-16	6.1	CVE-2024-9647
Tophive--Ultimate AI	The UltimateAI plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.8.3. This is due to the improper empty value check and a missing default activated value check in the 'ultimate_ai_change_pass' function. This makes it possible for unauthenticated attackers to reset the password of the first user, whose account is not yet activated or the first user who activated their account, who are subscribers.	2024-10-16	5.6	CVE-2024-9104
tychesoftwares--Arconix Shortcodes	The Arconix Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'button' shortcode in all versions up to, and including, 2.1.12 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-18	6.4	CVE-2024-9703
vercel--next.js	Next.js is a React Framework for the Web. Cersions on the 10.x, 11.x, 12.x, 13.x, and 14.x branches before version 14.2.7 contain a vulnerability in the image optimization feature which allows for a potential Denial of Service (DoS) condition which could lead to excessive CPU consumption. Neither the `next.config.js` file that is configured with `images.unoptimized` set to `true` or `images.loader` set to a non-default value nor the Next.js application that is hosted on Vercel are affected. This issue was fully patched in Next.js `14.2.7`. As a workaround, ensure that the `next.config.js` file has either `images.unoptimized`, `images.loader` or `images.loaderFile` assigned.	2024-10-14	5.9	CVE-2024-47831
VillaTheme--Email Template Customizer for WooCommerce	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in VillaTheme Email Template Customizer for WooCommerce allows Stored XSS.This issue affects Email Template Customizer for WooCommerce: from n/a through 1.2.5.	2024-10-17	5.9	CVE-2024-49288
vladolaru--Fonto Custom Web Fonts Manager	The Fonto - Custom Web Fonts Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-17	6.4	CVE-2024-8920
WAVLINK--WN530H4	A vulnerability was found in WAVLINK WN530H4, WN530HG4 and WN572HG3 up to 20221028 and classified as critical. This issue affects the function ping_ddns of the file internet.cgi. The manipulation of the argument DDNS leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-20	4.7	CVE-2024-10193
Weblizar--Lightbox slider Responsive	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Weblizar Lightbox slider - Responsive Lightbox Gallery	2024-10-17	6.5	CVE-2024-49280

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Lightbox Gallery	allows Stored XSS.This issue affects Lightbox slider - Responsive Lightbox Gallery: from n/a through 1.10.0.			
wepic--Country Flags for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wepic Country Flags for Elementor allows Stored XSS.This issue affects Country Flags for Elementor: from n/a through 1.0.1.	2024-10-17	6.5	CVE-2024-49262
WhileTrue--Most And Least Read Posts Widget	Cross-Site Request Forgery (CSRF) vulnerability in WhileTrue Most And Least Read Posts Widget allows Cross Site Request Forgery.This issue affects Most And Least Read Posts Widget: from n/a through 2.5.18.	2024-10-20	4.3	CVE-2024-49628
WisdmLabs--Edwiser Bridge	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WisdmLabs Edwiser Bridge allows Stored XSS.This issue affects Edwiser Bridge: from n/a through 3.0.7.	2024-10-17	6.5	CVE-2024-49311
WisdmLabs--Edwiser Bridge	Server-Side Request Forgery (SSRF) vulnerability in WisdmLabs Edwiser Bridge.This issue affects Edwiser Bridge: from n/a through 3.0.7.	2024-10-17	4.9	CVE-2024-49312
withastro--astro	The Astro web framework has a DOM Clobbering gadget in the client-side router starting in version 3.0.0 and prior to version 4.16.1. It can lead to cross-site scripting (XSS) in websites enables Astro's client-side routing and has *stored* attacker-controlled scriptless HTML elements (i.e., `iframe` tags with unsanitized `name` attributes) on the destination pages. This vulnerability can result in cross-site scripting (XSS) attacks on websites that built with Astro that enable the client-side routing with `ViewTransitions` and store the user-inserted scriptless HTML tags without properly sanitizing the `name` attributes on the page. Version 4.16.1 contains a patch for this issue.	2024-10-14	5.9	CVE-2024-47885
woocommerce -- woocommerce	The WooCommerce plugin for WordPress is vulnerable to HTML Injection in all versions up to, and including, 9.0.2. This is due to the plugin not properly neutralizing HTML elements from submitted order forms. This makes it possible for unauthenticated attackers to inject arbitrary HTML that will render when the administrator views order form submissions.	2024-10-15	6.1	CVE-2024-9944
WooCommerce--Product Vendors	The Product Vendors is vulnerable to Reflected Cross-Site Scripting via the 'vendor_description' parameter in versions up to, and including, 2.0.35 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-16	4.7	CVE-2017-20193
WooCommerce--WooCommerce Smart Coupons	The WooCommerce Smart Coupons plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the woocommerce_coupon_admin_init function in versions up to, and including, 4.6.0. This makes it possible for unauthenticated attackers to send themselves gift certificates of any value, which could be redeemed for products sold on the victim's storefront.	2024-10-16	5.3	CVE-2020-36841
WordPress Foundation--WordPress	WordPress Core, in versions up to 6.0.2, is vulnerable to Authenticated Stored Cross-Site Scripting that can be exploited by users with access to the WordPress post and page editor, typically consisting of Authors, Contributors, and Editors making it possible to inject arbitrary web scripts into posts and pages that execute if the the_meta(); function is called on that page.	2024-10-16	4.9	CVE-2022-4973

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WP-buy--WP Content Copy Protection & No Right Click	Cross-Site Request Forgery (CSRF) vulnerability in WP-buy WP Content Copy Protection & No Right Click allows Cross Site Request Forgery.This issue affects WP Content Copy Protection & No Right Click: from n/a through 3.5.9.	2024-10-20	4.3	CVE-2024-49306
wp-slimstat -- slimstat_analytics	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the resource parameter in all versions up to, and including, 5.2.6 due to insufficient input sanitization and output escaping when logging visitor requests. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-15	6.1	CVE-2024-9548
wpdevteam--Essential Addons for Elementor Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders	The Essential Addons for Elementor plugin for WordPress is vulnerable to authorization bypass in versions up to and including 4.6.4 due to missing capability checks and nonce disclosure. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to perform many unauthorized actions such as changing settings and installing arbitrary plugins.	2024-10-16	6.3	CVE-2021-4446
wpdiscover--Photo Gallery Builder	Subscriber Broken Access Control in Photo Gallery Builder <= 3.0 versions.	2024-10-20	4.3	CVE-2024-49325
wpextended--The Ultimate WordPress Toolkit WP Extended	The The Ultimate WordPress Toolkit - WP Extended plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'wpext-export' parameter in all versions up to, and including, 3.0.9 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-17	6.1	CVE-2024-9347
wpindeed--Indeed Membership Pro	The Indeed Membership Pro plugin for WordPress is vulnerable to authorization bypass due to missing capability checks on various AJAX actions in versions 7.3 - 8.6. This makes it possible for authenticated attacker, with minimal permission, such as a subscriber, to perform a variety of actions such as modifying settings and viewing sensitive data.	2024-10-16	6.3	CVE-2020-36833
wpmudev--Forminator Forms Contact Form, Payment Form & Custom Form Builder	The Forminator Forms - Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.35.1. This is due to missing or incorrect nonce validation on the quiz 'create_module' function. This makes it possible for unauthenticated attackers to create draft quizzes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-10-17	4.3	CVE-2024-9351
wpmudev--Forminator Forms Contact Form, Payment Form & Custom Form Builder	The Forminator Forms - Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.35.1. This is due to missing or incorrect nonce validation on the custom form 'create_module' function. This makes it possible for unauthenticated attackers to create draft forms via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-10-17	4.3	CVE-2024-9352
wproyal--Royal Elementor Addons and	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.3.986 via the	2024-10-17	4.3	CVE-2024-7417

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Templates	data_fetch. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract data from password protected posts.			
wpvividplugins--Migration, Backup, Staging WPvivid	The Migration, Backup, Staging - WPvivid plugin for WordPress is vulnerable to sensitive information disclosure of a WordPress site's database due to missing capability checks on the wp_ajax_wpvivid_add_remote AJAX action that allows low-level authenticated attackers to send back-ups to a remote location of their choice for review. This affects versions up to, and including 0.9.35.	2024-10-16	4.9	CVE-2020-36835
WPWeb--Social Auto Poster	Cross-Site Request Forgery (CSRF) vulnerability in WPWeb Social Auto Poster allows Cross Site Request Forgery.This issue affects Social Auto Poster: from n/a through 5.3.15.	2024-10-20	4.3	CVE-2024-49272
wpzest--Easy Menu Manager | WPZest	The Easy Menu Manager | WPZest plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-18	6.4	CVE-2024-9366
wpzita--Zita Elementor Site Library	The Zita Elementor Site Library plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.6.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-16	6.4	CVE-2024-8921
xplodedthemes -- wpide	The WPIDE - File Manager & Code Editor plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.4.9. This is due to the plugin utilizing the PHP-Parser library, which outputs parser rebuild command execution results. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	2024-10-15	5.3	CVE-2024-9546
zaytech -- smart_online_order_for_clover	The Smart Online Order for Clover plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's moo_receipt_link shortcode in all versions up to, and including, 1.5.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-15	5.4	CVE-2024-9895
zluck--Multiline files upload for contact form 7	The Multiline files upload for contact form 7 plugin for WordPress is vulnerable to unauthorized plugin deactivation due to a missing capability check on the mfcf7_zl_custom_handle_deactivation_plugin_form_submission() function in all versions up to, and including, 2.8.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to deactivate the plugin and send a custom reason from the site.	2024-10-16	4.3	CVE-2024-9891

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
archerirm -- archer	Archer Platform 2024.03 before version 2024.08 is affected by an authorization bypass vulnerability related to supporting application files. A remote unprivileged attacker could potentially exploit this vulnerability to elevate their privileges and delete system icons.	2024-10-22	3.1	CVE-2024-49208
code-projects--Blood Bank Management System	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /bloodrequest.php. The manipulation of the argument msg leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-27	3.5	CVE-2024-10419
Dell--Data Lakehouse	Dell Data Lakehouse, version(s) 1.0.0.0 and 1.1.0.0, contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2024-10-25	2.9	CVE-2024-47483
HCL Software--Sametime	HCL Sametime is impacted by the error messages containing sensitive information. An attacker can use this information to launch another, more focused attack.	2024-10-23	3.6	CVE-2023-50355
ibm -- concert	IBM Concert 1.0.0 and 1.0.1 vulnerable to attacks that rely on the use of cookies without the SameSite attribute.	2024-10-22	3.7	CVE-2024-43173
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: don't use rate mask for offchannel TX either Like the commit ab9177d83c04 ("wifi: mac80211: don't use rate mask for scanning"), ignore incorrect settings to avoid no supported rate warning reported by syzbot. The syzbot did bisect and found cause is commit 9df66d5b9f45 ("cfg80211: fix default HE tx bitrate mask in 2G band"), which however corrects bitmask of HE MCS and recognizes correctly settings of empty legacy rate plus HE MCS rate instead of returning -EINVAL. As suggestions [1], follow the change of SCAN TX to consider this case of offchannel TX as well. [1] https://lore.kernel.org/linux-wireless/6ab2dc9c3afe753ca6fdcdd1421e7a1f47e87b84.camel@sipsolutions.net/T/#m2ac2a6d2be06a37c9c47a3d8a44b4f647ed4f024	2024-10-21	3.3	CVE-2024-47738
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: RFCOMM: FIX possible deadlock in rfcomm_sk_state_change rfcomm_sk_state_change attempts to use sock_lock so it must never be called with it locked but rfcomm_sock_ioctl always attempt to lock it causing the following trace: ========== WARNING: possible circular locking dependency detected 6.8.0-syzkaller-08951-gfe46a7dd189e #0 Not tainted ---------- syz-executor386/5093 is trying to acquire lock: ffff88807c396258 (sk_lock-AF_BLUETOOTH-BTPROTO_RFCOMM){+.+.}-{0:0}, at: lock_sock include/net/sock.h:1671 [inline] ffff88807c396258 (sk_lock-AF_BLUETOOTH-BTPROTO_RFCOMM){+.+.}-{0:0}, at: rfcomm_sk_state_change+0x5b/0x310 net/bluetooth/rfcomm/sock.c:73 but task is already holding lock: ffff88807badfd28 (&d->lock){+.+.}-{3:3}, at: __rfcomm_dlc_close+0x226/0x6a0 net/bluetooth/rfcomm/core.c:491	2024-10-21	3.3	CVE-2024-50044
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: usb: typec: tipd: Free IRQ only if it was requested before In polling mode, if no IRQ was requested there is no need to free it. Call devm_free_irq() only if client->irq is set. This fixes the warning caused by the tps6598x module removal: WARNING: CPU: 2 PID: 333 at kernel/irq/devres.c:144 devm_free_irq+0x80/0x8c ... ... Call trace: devm_free_irq+0x80/0x8c tps6598x_remove+0x28/0x88 [tps6598x] i2c_device_remove+0x2c/0x9c device_remove+0x4c/0x80 device_release_driver_internal+0x1cc/0x228 driver_detach+0x50/0x98	2024-10-21	3.3	CVE-2024-50057

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bus_remove_driver+0x6c/0xbc driver_unregister+0x30/0x60 i2c_del_driver+0x54/0x64 tps6598x_i2c_driver_exit+0x18/0xc3c [tps6598x] __arm64_sys_delete_module+0x184/0x264 invoke_syscall+0x48/0x110 el0_svc_common.constprop.0+0xc8/0xe8 do_el0_svc+0x20/0x2c el0_svc+0x28/0x98 el0t_64_sync_handler+0x13c/0x158 el0t_64_sync+0x190/0x194			
PHPGurukul--Vehicle Record System	A vulnerability, which was classified as problematic, was found in PHPGurukul Vehicle Record System 1.0. This affects an unknown part of the file /admin/edit-brand.php. The manipulation of the argument Brand Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions the parameter "phone_number" to be affected. But this might be a mistake because the textbox field label is "Brand Name".	2024-10-27	2.4	CVE-2024-10414
Poco-z--Guns-Medical	A vulnerability was found in Poco-z Guns-Medical 1.0. It has been declared as problematic. Affected by this vulnerability is the function upload of the file /mgr/upload of the component File Upload. The manipulation of the argument picture leads to cross site scripting. The attack can be launched remotely.	2024-10-27	3.5	CVE-2024-10412
SourceCodester--Best House Rental Management System	A vulnerability was found in SourceCodester Best House Rental Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /index.php?page=tenants of the component Manage Tenant Details. The manipulation of the argument Last Name/First Name/Middle Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only shows the field "Last Name" to be affected. Other fields might be affected as well.	2024-10-24	3.5	CVE-2024-10348
Tektronix--Sentry	A vulnerability has been found in Tektronix Sentry 6.0.9 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /?page=reports of the component Reports Page. The manipulation of the argument z leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-23	3.5	CVE-2024-10276
umbraco -- umbraco_cms	Umbraco, a free and open source .NET content management system, has an insufficient session expiration issue in versions on the 13.x branch prior to 13.5.2, 10.x prior to 10.8.7, and 8.x prior to 8.18.15. The Backoffice displays the logout page with a session timeout message before the server session has fully expired, causing users to believe they have been logged out approximately 30 seconds before they actually are. Versions 13.5.2, 10.8,7, and 8.18.15 contain a patch for the issue.	2024-10-22	3.1	CVE-2024-48926
Admidio--admidio	Admidio is an open-source user management solution. Prior to version 4.3.12, an unsafe deserialization vulnerability allows any unauthenticated user to execute arbitrary code on the server. Version 4.3.12 fixes this issue.	2024-10-16	3.5	CVE-2024-47836
authzed -- spicedb	SpiceDB is an open source database for scalably storing and querying fine-grained authorization data. Starting in version 1.35.0 and prior to version 1.37.1, clients that have enabled `LookupResources2` and have caveats in the evaluation path for their requests can return a permissionship of `CONDITIONAL` with context marked as missing, even then the context was supplied. LookupResources2 is the new default in SpiceDB 1.37.0 and has been opt-in since SpiceDB 1.35.0. The bug is patched as part of SpiceDB 1.37.1. As a workaround, disable LookupResources2 via the `--enable-experimental-lookup-resources` flag by setting it to `false`.	2024-10-14	2.4	CVE-2024-48909
code-projects--Blood Bank	A vulnerability has been found in code-projects Blood Bank System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /viewrequest.php. The manipulation leads to cross site scripting. The attack can	2024-10-19	3.5	CVE-2024-10142

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
System	be initiated remotely. The exploit has been disclosed to the public and may be used.			
Eclipse Foundation--Jetty	Jetty PushSessionCacheFilter can be exploited by unauthenticated users to launch remote DoS attacks by exhausting the server's memory.	2024-10-14	3.1	CVE-2024-6762
Eclipse Foundation--Jetty	Eclipse Jetty is a lightweight, highly scalable, Java-based web server and Servlet engine . It includes a utility class, HttpURI, for URI/URL parsing. The HttpURI class does insufficient validation on the authority segment of a URI. However the behaviour of HttpURI differs from the common browsers in how it handles a URI that would be considered invalid if fully validated against the RRC. Specifically HttpURI and the browser may differ on the value of the host extracted from an invalid URI and thus a combination of Jetty and a vulnerable browser may be vulnerable to a open redirect attack or to a SSRF attack if the URI is used after passing validation checks.	2024-10-14	3.7	CVE-2024-6763
elabftw--elabftw	eLabFTW is an open source electronic lab notebook for research labs. A vulnerability in versions prior to 5.1.5 allows an attacker to inject arbitrary HTML tags in the pages: "experiments.php" (show mode), "database.php" (show mode) or "search.php". It works by providing HTML code in the extended search string, which will then be displayed back to the user in the error message. This means that injected HTML will appear in a red "alert/danger" box, and be part of an error message. Due to some other security measures, it is not possible to execute arbitrary javascript from this attack. As such, this attack is deemed low impact. Users should upgrade to at least version 5.1.5 to receive a patch. No known workarounds are available.	2024-10-14	3.5	CVE-2024-47826
jsbroks--COCO Annotator	A vulnerability, which was classified as problematic, was found in jsbroks COCO Annotator 0.11.1. This affects an unknown part of the component Session Handler. The manipulation of the argument SECRET_KEY leads to predictable from observable state. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used.	2024-10-19	3.7	CVE-2024-10141
oracle -- graalvm	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	2024-10-15	3.7	CVE-2024-21217
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.1	2024-10-15	3.1	CVE-2024-21231

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L).			
oracle -- mysql	Vulnerability in the MySQL Client product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Client accessible data as well as unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).	2024-10-15	3.8	CVE-2024-21247
oracle -- mysql	Vulnerability in the MySQL Client product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.1 Base Score 2.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N).	2024-10-15	2	CVE-2024-21209
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2024-10-15	2.2	CVE-2024-21232
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication GCS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2024-10-15	2.2	CVE-2024-21237
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Telemetry). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N).	2024-10-15	2.2	CVE-2024-21243
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Telemetry). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N).	2024-10-15	2.2	CVE-2024-21244
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM	2024-10-15	2.3	CVE-2024-21253

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 2.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).			
Oracle Corporation--GraalVM	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle Java SE: 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	2024-10-15	3.7	CVE-2024-21211
Oracle Corporation--Oracle Database Server	Vulnerability in the XML Database component of Oracle Database Server. Supported versions that are affected are 19.3-19.24, 21.3-21.15 and 23.4-23.5. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via HTTP to compromise XML Database. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of XML Database. CVSS 3.1 Base Score 3.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L).	2024-10-15	3.5	CVE-2024-21242
Oracle Corporation--Oracle Database Server	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.24, 21.3-21.15 and 23.4-23.5. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM accessible data. CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	2024-10-15	3.1	CVE-2024-21251
Oracle Corporation--Oracle Hyperion BI+	Vulnerability in the Oracle Hyperion BI+ product of Oracle Hyperion (component: UI and Visualization). The supported version that is affected is 11.2.18.0.000. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion BI+ executes to compromise Oracle Hyperion BI+. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion BI+ accessible data. CVSS 3.1 Base Score 3.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N).	2024-10-15	3	CVE-2024-21257
Oracle Corporation--Oracle Java SE	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to	2024-10-15	3.7	CVE-2024-21208

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).			
Oracle Corporation--Oracle Java SE	Vulnerability in Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4 and 23. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	2024-10-15	3.7	CVE-2024-21210
PHPGurukul--Boat Booking System	A vulnerability was found in PHPGurukul Boat Booking System 1.0. It has been classified as problematic. This affects an unknown part of the file book-boat.php?bid=1 of the component Book a Boat Page. The manipulation of the argument phone_number leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-19	3.5	CVE-2024-10155
PHPGurukul--Boat Booking System	A vulnerability, which was classified as problematic, was found in PHPGurukul Boat Booking System 1.0. This affects an unknown part of the file /admin/book-details.php of the component Booking Details Page. The manipulation of the argument Official Remark leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-20	3.5	CVE-2024-10191
PHPGurukul--IFSC Code Finder Project	A vulnerability has been found in PHPGurukul IFSC Code Finder Project 1.0 and classified as problematic. This vulnerability affects unknown code of the file search.php. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-20	3.5	CVE-2024-10192
splunk -- splunk	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403.108, and 9.1.2312.204, a low-privileged user that does not hold the "admin" or "power" Splunk roles could change the maintenance mode state of App Key Value Store (KVStore) through a Cross-Site Request Forgery (CSRF).	2024-10-14	3.5	CVE-2024-45737
Topdata--Inner Rep Plus WebServer	A vulnerability was found in Topdata Inner Rep Plus WebServer 2.01. It has been classified as problematic. Affected is an unknown function of the file /InnerRepPlus.html of the component Operator Details Form. The manipulation leads to missing password field masking. It is possible to launch the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-18	2.7	CVE-2024-10122
Topdata--Inner Rep Plus WebServer	A vulnerability was found in Topdata Inner Rep Plus WebServer 2.01. It has been rated as problematic. Affected by this issue is some unknown functionality of the file td.js.gz. The manipulation leads to risky cryptographic algorithm. The attack may be launched remotely. The exploit has been disclosed to the public and may	2024-10-18	2.7	CVE-2024-10128

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	be used. The vendor was contacted early about this disclosure but did not respond in any way.			
VMware--Spring	The fix for CVE-2022-22968 made disallowedFields patterns in DataBinder case insensitive. However, String.toLowerCase() has some Locale dependent exceptions that could potentially result in fields not protected as expected.	2024-10-18	3.1	CVE-2024-38820
vue--vue	Improper regular expression in Vue's parseHTML function leads to a potential regular expression denial of service vulnerability.	2024-10-15	3.7	CVE-2024-9506