BULLETIN (SB21-151)

VULNERABILITY SUMMARY FOR THE WEEK OF

24TH MAY, 2021

Bulletin (SB21-151)
Vulnerability Summary for the Week of May 24, 2021

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
aioseo -- all_in_one_seo	The All in One SEO – Best WordPress SEO Plugin – Easily Improve Your SEO Rankings before 4.1.0.2 enables authenticated users with "aioseo_tools_settings" privilege (most of the time admin) to execute arbitrary code on the underlying host. Users can restore plugin's configuration by uploading a backup .ini file in the section "Tool > Import/Export". However, the plugin attempts to unserialize values of the .ini file. Moreover, the plugin embeds Monolog library which can be used to craft a gadget chain and thus trigger system command execution.	2021-05-24	9	CVE-2021-24307 CONFIRM MISC
cisco -- dna_spaces\	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. These vulnerabilities are due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities by leveraging the insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin and execute arbitrary commands on the underlying operating system as root.	2021-05-22	7.2	CVE-2021-1558 CISCO
cisco -- dna_spaces\	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. These vulnerabilities are due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities by leveraging the insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin and execute arbitrary commands on the underlying operating system as root.	2021-05-22	7.2	CVE-2021-1557 CISCO
cisco -- dna_spaces\	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, remote attacker to perform a command injection attack on an affected device. These vulnerabilities are due to insufficient input sanitization when executing affected commands. A high-privileged attacker could exploit these vulnerabilities on a Cisco DNA Spaces Connector by injecting crafted input during command execution. A successful exploit could allow the attacker to execute arbitrary commands as root within the Connector docker container.	2021-05-22	9	CVE-2021-1560 CISCO
cisco -- dna_spaces\	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, remote attacker to perform a command injection attack on an affected device. These vulnerabilities are due to insufficient input sanitization when executing affected commands. A high-privileged attacker could exploit these vulnerabilities on a Cisco DNA Spaces Connector by injecting crafted input during command execution. A successful exploit could allow the attacker to execute arbitrary commands as root within the Connector docker container.	2021-05-22	9	CVE-2021-1559 CISCO
cisco -- evolved_programmable_network_manager	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Evolved Programmable Network (EPN) Manager could allow an authenticated, remote attacker to execute arbitrary commands on an affected system. The vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the interface. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system (OS) with the permissions of a special non-root user. In this way, an attacker could take control of the affected system, which would allow them to obtain and alter sensitive data. The attacker could also affect the devices that are managed by the affected system by pushing arbitrary configuration files, retrieving device credentials	2021-05-22	9	CVE-2021-1487 CISCO

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and confidential information, and ultimately undermining the stability of the devices, causing a denial of service (DoS) condition.			
cisco -- modeling_labs	A vulnerability in the web UI of Cisco Modeling Labs could allow an authenticated, remote attacker to execute arbitrary commands with the privileges of the web application on the underlying operating system of an affected Cisco Modeling Labs server. This vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected server. A successful exploit could allow the attacker to execute arbitrary commands with the privileges of the web application, virl2, on the underlying operating system of the affected server. To exploit this vulnerability, the attacker must have valid user credentials on the web UI.	2021-05-22	9	CVE-2021-1531 CISCO
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1550 CISCO
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1555 CISCO
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1554 CISCO
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1553 CISCO

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1552 CISCO
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1551 CISCO
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1548 CISCO
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1549 CISCO
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1547 CISCO
codesys -- v2_runtime_system_sp	CODESYS V2 runtime system SP before 2.4.7.55 has a Stack-based Buffer Overflow.	2021-05-25	7.5	CVE-2021-30188 MISC MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codesys -- v2_web_server	CODESYS V2 Web-Server before 1.1.9.20 has a Stack-based Buffer Overflow.	2021-05-25	7.5	CVE-2021-30189 MISC MISC
codesys -- v2_web_server	CODESYS V2 Web-Server before 1.1.9.20 has Improper Access Control.	2021-05-25	7.5	CVE-2021-30190 MISC MISC
codesys -- v2_web_server	CODESYS V2 Web-Server before 1.1.9.20 has an Improperly Implemented Security Check.	2021-05-25	7.5	CVE-2021-30192 MISC MISC
codesys -- v2_web_server	CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Write.	2021-05-25	7.5	CVE-2021-30193 MISC MISC
college_management_system_project -- college_management_system	Projectsworlds College Management System Php 1.0 is vulnerable to SQL injection issues over multiple parameters.	2021-05-24	7.5	CVE-2020-25409 MISC MISC
deep-defaults_project -- deep-defaults	Prototype pollution vulnerability in 'deep-defaults' versions 1.0.0 through 1.0.5 allows attacker to cause a denial of service and may lead to remote code execution.	2021-05-25	7.5	CVE-2021-25944 MISC
eyesofnetwork -- eyesofnetwork	EyesOfNetwork eonweb through 5.3-11 allows Remote Command Execution (by authenticated users) via shell metacharacters in the nagios_path parameter to lilac/export.php, as demonstrated by %26%26+curl to insert an "&& curl" substring for the shell.	2021-05-24	9	CVE-2021-33525 MISC MISC
ibm -- security_guardium	IBM Security Guardium 11.2 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 195766.	2021-05-24	9	CVE-2021-20385 CONFIRM XF
ibm -- security_guardium	IBM Security Guardium 11.2 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 199184.	2021-05-24	9	CVE-2021-20557 XF CONFIRM
ibm -- security_guardium	IBM Security Guardium 11.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 196313.	2021-05-24	7.5	CVE-2021-20426 CONFIRM XF
linux -- linux_kernel	This vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel 5.11.15. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of eBPF programs. The issue results from the lack of proper validation of user-supplied eBPF programs prior to executing them. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel. Was ZDI-CAN-13661.	2021-05-21	7.2	CVE-2021-31440 MISC MISC
nagios -- fusion	Insufficient Verification of Data Authenticity in Nagios Fusion 4.1.8 and earlier and Nagios XI 5.7.5 and earlier allows for Escalation of Privileges or Code Execution as root via vectors related to an untrusted update package to upgrade_to_latest.sh.	2021-05-24	10	CVE-2020-28900 MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
nagios -- fusion	Command Injection in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation to nagios.	2021-05-24	7.5	CVE-2020-28908 MISC MISC MISC
nagios -- fusion	Command Injection in Nagios Fusion 4.1.8 and earlier allows Privilege Escalation from apache to root in cmd_subsys.php.	2021-05-24	10	CVE-2020-28902 MISC MISC MISC
nagios -- fusion	Incorrect SSL certificate validation in Nagios Fusion 4.1.8 and earlier allows for Escalation of Privileges or Code Execution as root via vectors related to download of an untrusted update package in upgrade_to_latest.sh.	2021-05-24	10	CVE-2020-28907 MISC MISC MISC
nagios -- fusion	Incorrect File Permissions in Nagios XI 5.7.5 and earlier and Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation to root. Low-privileged users are able to modify files that are included (aka sourced) by scripts executed by root.	2021-05-24	9	CVE-2020-28906 MISC MISC MISC
nagios -- fusion	Command Injection in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation or Code Execution as root via vectors related to corrupt component installation in cmd_subsys.php.	2021-05-24	10	CVE-2020-28901 MISC MISC MISC
nagios -- fusion	Incorrect File Permissions in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation to root via modification of scripts. Low-privileges users are able to modify files that can be executed by sudo.	2021-05-24	9	CVE-2020-28909 MISC MISC MISC
nagios -- fusion	Execution with Unnecessary Privileges in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation as nagios via installation of a malicious component containing PHP code.	2021-05-24	7.5	CVE-2020-28904 MISC MISC MISC
nagios -- nagios_xi	Creation of a Temporary Directory with Insecure Permissions in Nagios XI 5.7.5 and earlier allows for Privilege Escalation via creation of symlinks, which are mishandled in getprofile.sh.	2021-05-24	10	CVE-2020-28910 MISC MISC MISC
nconf-toml_project -- nconf-toml	Prototype pollution vulnerability in `nconf-toml` versions 0.0.1 through 0.0.2 allows an attacker to cause a denial of service and may lead to remote code execution.	2021-05-25	7.5	CVE-2021-25946 MISC MISC
netgear -- gc108p_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before	2021-05-21	10	CVE-2021-33514 MISC MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3.			
plone -- plone	Plone through 5.2.4 allows remote authenticated managers to perform disk I/O via crafted keyword arguments to the ReStructuredText transform in a Python script.	2021-05-21	8.5	CVE-2021-33509 MISC MLIST
re-logic -- terraria	Re-Logic Terraria before 1.4.2.3 performs Insecure Deserialization.	2021-05-24	7.5	CVE-2021-32075 MISC MISC MISC MISC
ronomon -- opened	The @ronomon/opened library before 1.5.2 is vulnerable to a command injection vulnerability which would allow a remote attacker to execute commands on the system if the library was used with untrusted input.	2021-05-24	10	CVE-2021-29300 MISC CONFIRM
solarwinds -- network_performance_monitor	This vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Network Performance Monitor 2020.2.1. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SolarWinds.Serialization library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-12213.	2021-05-21	10	CVE-2021-31474 MISC MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. A heap-based buffer overflow in function WebPDecodeRGBInto is possible due to an invalid check for buffer size. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	7.5	CVE-2020-36328 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. A use-after-free was found due to a thread being killed too early. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	7.5	CVE-2020-36329 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. An unitialized variable is used in function ReadSymbol. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	7.5	CVE-2018-25014 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. A heap-based buffer overflow was found in PutLE16(). The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	7.5	CVE-2018-25011 MISC
zephyrproject -- zephyr	Possible read out of bounds in dns read. Zephyr versions >= 1.14.2, >= 2.3.0 contain Out-of-bounds Read (CWE-125). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-mm57-9hqw-qh44	2021-05-25	7.5	CVE-2020-13601 MISC
zephyrproject -- zephyr	Improper Input Frame Validation in ieee802154 Processing. Zephyr versions >= v1.14.2, >= v2.2.0 contain Stack-based Buffer Overflow (CWE-121), Heap-based Buffer Overflow (CWE-122). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-3gvq-h42f-v3c7	2021-05-25	7.5	CVE-2020-10064 MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zzcms -- zzcms	An issue was discovered in zzcms 2019. SQL Injection exists in user/ztconfig.php via the daohang or img POST parameter.	2021-05-24	7.5	CVE-2019-12348 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acronis -- true_image_2020	An issue was discovered in Acronis True Image 2020 24.5.22510. anti_ransomware_service.exe exposes a REST API that can be used by everyone, even unprivileged users. This API is used to communicate from the GUI to anti_ransomware_service.exe. This can be exploited to add an arbitrary malicious executable to the whitelist, or even exclude an entire drive from being monitored by anti_ransomware_service.exe.	2021-05-25	4.6	CVE-2020-9450 MISC MISC MISC
arangodb -- arangodb	In ArangoDB, versions v2.2.6.2 through v3.7.10 are vulnerable to Cross-Site Scripting (XSS), since there is no validation of the .zip file name and filtering of potential abusive characters which zip files can be named to. There is no X-Frame-Options Header set, which makes it more susceptible for leveraging self XSS by attackers.	2021-05-24	4.3	CVE-2021-25938 MISC MISC
bitdefender -- endpoint_security_tools	An Improper Input Validation vulnerability in the Product Update feature of Bitdefender Endpoint Security Tools for Linux allows a man-in-the-middle attacker to abuse the DownloadFile function of the Product Update to achieve remote code execution. This issue affects: Bitdefender Endpoint Security Tools for Linux versions prior to 6.2.21.155.	2021-05-24	6	CVE-2021-3485 MISC
bludit -- bludit	A file upload vulnerability was discovered in the file path /bl-plugins/backup/plugin.php on Bludit version 3.12.0. If an attacker is able to gain Administrator rights they will be able to use unsafe plugins to upload a backup file and control the server.	2021-05-21	6.5	CVE-2020-23765 MISC
boostifythemes -- goto	The Goto WordPress theme before 2.1 did not properly sanitize the formvalue JSON POST parameter in its tl_filter AJAX action, leading to an unauthenticated Reflected Cross-site Scripting (XSS) vulnerability.	2021-05-24	4.3	CVE-2021-24297 CONFIRM
calendar01_project -- calendar01	Reflected cross-site scripting vulnerability in the admin page of [Calendar01] free edition ver1.0.1 and earlier allows a remote attacker to inject an arbitrary script via unspecified vectors.	2021-05-24	4.3	CVE-2021-20725 MISC MISC
cisco -- finesse	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to redirect a user to an undesired web page. This vulnerability is due to improper input validation of the URL parameters in an HTTP request that is sent to an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to cause the interface to redirect the user to a specific, malicious	2021-05-22	5.8	CVE-2021-1358 CISCO

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	URL. This type of vulnerability is known as an open redirect and is used in phishing attacks that get users to unknowingly visit malicious sites.			
cisco -- finesse	Multiple vulnerabilities in the web-based management interface of Cisco Finesse could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit these vulnerabilities by injecting malicious code into the web-based management interface and persuading a user to click a malicious 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. An attacker needs valid administrator credentials to inject the malicious script code.	2021-05-22	4.3	CVE-2021-1254 CISCO
codesys -- plcwinnt	CODESYS V2 runtime system before 2.4.7.55 has Improper Input Validation.	2021-05-25	5	CVE-2021-30195 MISC MISC
codesys -- plcwinnt	CODESYS V2 runtime system SP before 2.4.7.55 has a Heap-based Buffer Overflow.	2021-05-25	5	CVE-2021-30186 MISC MISC
codesys -- runtime_toolkit	CODESYS V2 runtime system SP before 2.4.7.55 has Improper Neutralization of Special Elements used in an OS Command.	2021-05-25	4.6	CVE-2021-30187 MISC MISC
codesys -- v2_web_server	CODESYS V2 Web-Server before 1.1.9.20 has a a Buffer Copy without Checking the Size of the Input.	2021-05-25	5	CVE-2021-30191 MISC MISC
codesys -- v2_web_server	CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Read.	2021-05-25	6.4	CVE-2021-30194 MISC MISC
college_management_system_project -- college_management_system	A Cross-Site Request Forgery (CSRF) vulnerability exists in ProjectWorlds College Management System Php 1.0 that allows a remote attacker to modify, delete, or make a new entry of the student, faculty, teacher, subject, scores, location, and article data.	2021-05-24	4.3	CVE-2020-25408 MISC MISC
dell -- xtremio_management_server	Dell EMC XtremIO Versions prior to 6.3.3-8, contain a Cross-Site Request Forgery Vulnerability in XMS. A non-privileged attacker could potentially exploit this vulnerability, leading to a privileged victim application user being tricked into sending state-changing requests to the vulnerable application, causing unintended server operations.	2021-05-21	6.8	CVE-2021-21549 CONFIRM
dutchcoders -- transfer.sh	Dutchcoders transfer.sh before 1.2.4 allows XSS via an inline view.	2021-05-24	4.3	CVE-2021-33496 MISC CONFIRM MISC MISC
dutchcoders -- transfer.sh	Dutchcoders transfer.sh before 1.2.4 allows Directory Traversal for deleting files.	2021-05-24	6.4	CVE-2021-33497 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM MISC
emlog -- emlog	An issue was discovered in emlog 6.0.0stable. There is a SQL Injection vulnerability that can execute any SQL statement and query server sensitive data via admin/navbar.php?action=add_page.	2021-05-24	6.5	CVE-2021-30081 MISC
feehi -- feehi_cms	Feehi CMS 2.1.1 is affected by a Server-side request forgery (SSRF) vulnerability. When the user modifies the HTTP Referer header to any url, the server can make a request to it.	2021-05-24	6.4	CVE-2021-30108 MISC
ffmpeg -- ffmpeg	A heap-based Buffer Overflow Vulnerability exists FFmpeg 4.2 at libavfilter/vf_vmafmotion.c in convolution_y_8bit, which could let a remote malicious user cause a Denial of Service.	2021-05-27	4.3	CVE-2020-22033 MISC
ffmpeg -- ffmpeg	FFmpeg 4.2 is affected by null pointer dereference passed as argument to libavformat/aviobuf.c, which could cause a Denial of Service.	2021-05-25	5	CVE-2020-20450 MISC
ffmpeg -- ffmpeg	FFmpeg 4.2 is affected by a Divide By Zero issue via libavcodec/lpc.h, which allows a remote malicious user to cause a Denial of Service.	2021-05-25	4	CVE-2020-20445 MISC
ffmpeg -- ffmpeg	FFmpeg 4.2 is affected by a Divide By Zero issue via libavcodec/aacpsy.c, which allows a remote malicious user to cause a Denial of Service.	2021-05-25	4	CVE-2020-20446 MISC
ffmpeg -- ffmpeg	FFmpeg 4.1.3 is affected by a Divide By Zero issue via libavcodec/ratecontrol.c, which allows a remote malicious user to cause a Denial of Service.	2021-05-25	4	CVE-2020-20448 MISC
ffmpeg -- ffmpeg	FFmpeg 4.2 is affected by a Divide By Zero issue via libavcodec/aaccoder, which allows a remote malicious user to cause a Denial of Service	2021-05-25	4	CVE-2020-20453 MISC
ffmpeg -- ffmpeg	Buffer Overflow vulnerability exists in FFmpeg 4.1 via apng_do_inverse_blend in libavcodec/pngenc.c, which could let a remote malicious user cause a Denial of Service	2021-05-24	5	CVE-2020-21041 MISC
ffmpeg -- ffmpeg	Denial of Service issue in FFmpeg 4.2 due to resource management errors via fftools/cmdutils.c.	2021-05-25	5	CVE-2020-20451 MISC
ffmpeg -- ffmpeg	A heap-based Buffer Overflow vulnerability exists FFmpeg 4.2 atlibavfilter/vf_floodfill.c, which might lead to memory corruption and other potential consequences.	2021-05-27	6.8	CVE-2020-22034 MISC
ffmpeg -- ffmpeg	Buffer Overflow vulnerability in FFMpeg 4.2.3 in dnn_execute_layer_pad in libavfilter/dnn/dnn_backend_native_layer_pad.c due to a call to memcpy without length checks, which could let a remote malicious user execute arbitrary code.	2021-05-26	6.5	CVE-2020-24020 MISC MISC
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the browseForDoc function. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13523.	2021-05-21	6.8	CVE-2021-31473 MISC MISC
gnome -- gupnp	An issue was discovered in GUPnP before 1.0.7 and 1.1.x and 1.2.x before 1.2.5. It allows DNS rebinding. A remote web server can exploit this	2021-05-24	5.8	CVE-2021-33516

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability to trick a victim's browser into triggering actions against local UPnP services implemented using this library. Depending on the affected service, this could be used for data exfiltration, data tempering, etc.			MISC MISC
gris_cms_project -- gris_cms	An issue was discovered in Gris CMS v0.1. There is a Persistent XSS vulnerability which allows remote attackers to inject arbitrary web script or HTML via admin/dashboard.	2021-05-24	4.3	CVE-2021-30082 MISC
htmly -- htmly	An arbitrary file deletion vulnerability was discovered on htmly v2.7.5 which allows remote attackers to use any absolute path to delete any file in the server should they gain Administrator privileges.	2021-05-21	5.5	CVE-2020-23766 MISC
ibenic -- simple_giveaways	The method and share GET parameters of the Giveaway pages were not sanitised, validated or escaped before being output back in the pages, thus leading to reflected XSS	2021-05-24	4.3	CVE-2021-24298 MISC CONFIRM
ibm -- 8335-gca_firmware	IBM Host firmware for LC-class Systems is vulnerable to a stack based buffer overflow, caused by improper bounds checking. A remote privileged attacker could exploit this vulnerability and cause a denial of service. IBM X-Force ID: 190037.	2021-05-25	4	CVE-2020-4839 CONFIRM XF
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 could allow an attacker to obtain sensitive information by injecting parameters into an HTML query. This information could be used in further attacks against the system. IBM X-Force ID: 199918.	2021-05-21	5	CVE-2021-29681 XF CONFIRM
ibm -- security_guardium	IBM Security Guardium 11.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 196280.	2021-05-24	5	CVE-2021-20419 CONFIRM XF
ibm -- security_guardium	IBM Security Guardium 11.2 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 192710.	2021-05-24	6.5	CVE-2020-4990 CONFIRM XF
ibm -- security_guardium	IBM Security Guardium 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195767.	2021-05-24	4.3	CVE-2021-20386 CONFIRM XF
ibm -- security_guardium	IBM Security Guardium 11.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196315.	2021-05-24	5	CVE-2021-20428 CONFIRM XF
jenkins -- urltrigger	Jenkins URLTrigger Plugin 0.48 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2021-05-25	5.5	CVE-2021-21659 CONFIRM MLIST
joomla -- joomla\!	An issue was discovered in Joomla! 3.0.0 through 3.9.26. A missing token check causes a CSRF vulnerability in data download endpoints in com_banners and com_sysinfo.	2021-05-26	4.3	CVE-2021-26034 MISC
joomla -- joomla\!	An issue was discovered in Joomla! 3.0.0 through 3.9.26. A missing token check causes a CSRF vulnerability in the AJAX reordering endpoint.	2021-05-26	4.3	CVE-2021-26033 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
joomla -- joomla\!	An issue was discovered in Joomla! 3.0.0 through 3.9.26. HTML was missing in the executable block list of MediaHelper::canUpload, leading to XSS attack vectors.	2021-05-26	4.3	CVE-2021-26032 MISC
linaro -- trusted_firmware-m	In Trusted Firmware-M through 1.3.0, cleaning up the memory allocated for a multi-part cryptographic operation (in the event of a failure) can prevent the abort() operation in the associated cryptographic library from freeing internal resources, causing a memory leak.	2021-05-21	5	CVE-2021-32032 CONFIRM MISC MISC
linux -- linux_kernel	A memory leak vulnerability was found in Linux kernel in llcp_sock_connect	2021-05-25	5	CVE-2020-25672 FEDORA MLIST FEDORA MISC FEDORA
lucyparsonslabs -- openoversight	Cross-site request forgery in OpenOversight 0.6.4 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link.	2021-05-25	5.8	CVE-2021-20096 MISC
mailform01_project -- mailform01	Reflected cross-site scripting vulnerability in [MailForm01] free edition (versions which the last updated date listed at the top of descriptions in the program file is from 2014 December 12 to 2018 July 27) allows a remote attacker to inject an arbitrary script via unspecified vectors.	2021-05-24	4.3	CVE-2021-20723 MISC MISC
mediateknet -- netwave_system	An information disclosure vulnerability was discovered in /index.class.php (via port 8181) on NetWave System 1.0 which allows unauthenticated attackers to exfiltrate sensitive information from the system.	2021-05-25	5	CVE-2021-27823 MISC MISC
metinfo -- metinfo	MetInfo 7.0 beta is affected by a file modification vulnerability. Attackers can delete and modify ini files in app/system/language/admin/language_general.class.php and app/system/include/function/file.func.php.	2021-05-24	6.4	CVE-2020-20907 MISC MISC
mlfactory -- dsgvo_all_in_one_for_wp	The dsgvoaio_write_log AJAX action of the DSGVO All in one for WP WordPress plugin before 4.0 did not sanitise or escape some POST parameter submitted before outputting them in the Log page in the administrator dashboard (wp-admin/admin.php?page=dsgvoaiofree-show-log). This could allow unauthenticated attackers to gain unauthorised access by using an XSS payload to create a rogue administrator account, which will be trigged when an administrator will view the logs.	2021-05-24	4.3	CVE-2021-24294 CONFIRM
nagios -- fusion	Incorrect Access Control in Nagios Fusion 4.1.8 and earlier allows low-privileged authenticated users to extract passwords used to manage fused servers via the test_server command in ajaxhelper.php.	2021-05-24	4	CVE-2020-28911 MISC MISC MISC
nagios -- fusion	Improper Input Validation in Nagios Fusion 4.1.8 and earlier allows an authenticated attacker to execute remote code via table pagination.	2021-05-24	6.5	CVE-2020-28905 MISC MISC MISC
nagios -- fusion	Improper input validation in Nagios Fusion 4.1.8 and earlier allows a remote attacker with control over a fused server to inject arbitrary HTML, aka XSS.	2021-05-24	4.3	CVE-2020-28903 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
nitrokey -- fido_u2f_firmware	An issue was discovered in Nitrokey FIDO U2F firmware through 1.1. Communication between the microcontroller and the secure element transmits credentials in plain. This allows an adversary to eavesdrop the communication and derive the secrets stored in the microcontroller. As a result, the attacker is able to arbitrarily manipulate the firmware of the microcontroller.	2021-05-21	5	CVE-2020-12061 MISC MISC MISC
normalize-url_project -- normalize-url	The normalize-url package before 4.5.1, 5.x before 5.3.1, and 6.x before 6.0.1 for Node.js has a ReDoS (regular expression denial of service) issue because it has exponential performance for data: URLs.	2021-05-24	5	CVE-2021-33502 CONFIRM
nsa -- emissary	Emissary is a distributed, peer-to-peer, data-driven workflow framework. Emissary 6.4.0 is vulnerable to Unsafe Deserialization of post-authenticated requests to the [`WorkSpaceClientEnqueue.action`](https://github.com/NationalSecurityAgency/emissary/blob/30c54ef16c6eb6ed09604a929939fb9f66868382/src/main/java/emissary/server/mvc/internal/WorkSpaceClientEnqueueAction.java) REST endpoint. This issue may lead to post-auth Remote Code Execution. This issue has been patched in version 6.5.0. As a workaround, one can disable network access to Emissary from untrusted sources.	2021-05-21	6.5	CVE-2021-32634 CONFIRM MISC
online_examination_system_project -- online_examination_system	Projectworlds Online Examination System 1.0 is vulnerable to CSRF, which allows a remote attacker to delete the existing user.	2021-05-24	4.3	CVE-2020-25411 MISC MISC
online_examination_system_project -- online_examination_system	Project Worlds Online Examination System 1.0 is affected by Cross Site Scripting (XSS) via account.php.	2021-05-24	4.3	CVE-2020-26006 MISC MISC
openid -- openid	It was found that various OpenID Providers (OPs) had TLS Server Certificates that used weak keys, as a result of the Debian Predictable Random Number Generator (CVE-2008-0166). In combination with the DNS Cache Poisoning issue (CVE-2008-1447) and the fact that almost all SSL/TLS implementations do not consult CRLs (currently an untracked issue), this means that it is impossible to rely on these OPs.	2021-05-21	4.3	CVE-2008-3280 MISC MISC
overwolf -- overwolf	Untrusted search path vulnerability in The Installer of Overwolf 2.168.0.n and earlier allows an attacker to gain privileges and execute arbitrary code with the privilege of the user invoking the installer via a Trojan horse DLL in an unspecified directory.	2021-05-24	4.4	CVE-2021-20726 MISC MISC
phpyun -- phpyun	An information disclosure vulnerability was discovered in alipay_function.php in the log file of Alibaba payment interface on PHPPYUN prior to version 5.0.1. If exploited, this vulnerability will allow attackers to obtain users' personally identifiable information including e-mail address and telephone numbers.	2021-05-21	5	CVE-2020-23768 MISC
pickplugins -- product_slider_for_woocommerce	The slider import search feature of the PickPlugins Product Slider for WooCommerce WordPress plugin before 1.13.22 did not properly sanitised the keyword GET parameter, leading to reflected Cross-Site Scripting issue	2021-05-24	4.3	CVE-2021-24300 CONFIRM
plone -- plone	Plone though 5.2.4 allows SSRF via the lxml parser. This affects Diazo themes, Dexterity TTW schemas, and modeleditors in plone.app.theming, plone.app.dexterity, and plone.supermodel.	2021-05-21	5	CVE-2021-33511 MISC MLIST

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
plone -- plone	Zope Products.CMFCore before 2.5.1 and Products.PluggableAuthService before 2.6.2, as used in Plone through 5.2.4 and other products, allow Reflected XSS.	2021-05-21	4.3	CVE-2021-33507 MISC MLIST
plone -- plone	Zope is an open-source web application server. In Zope versions prior to 4.6 and 5.2, users can access untrusted modules indirectly through Python modules that are available for direct use. By default, only users with the Manager role can add or edit Zope Page Templates through the web, but sites that allow untrusted users to add/edit Zope Page Templates through the web are at risk from this vulnerability. The problem has been fixed in Zope 5.2 and 4.6. As a workaround, a site administrator can restrict adding/editing Zope Page Templates through the web using the standard Zope user/role permission mechanisms. Untrusted users should not be assigned the Zope Manager role and adding/editing Zope Page Templates through the web should be restricted to trusted users only.	2021-05-21	6.5	CVE-2021-32633 MISC CONFIRM MLIST MLIST
plone -- plone	Plone through 5.2.4 allows remote authenticated managers to conduct SSRF attacks via an event ical URL, to read one line of a file.	2021-05-21	4	CVE-2021-33510 MISC MLIST
privoxy -- privoxy	A memory leak vulnerability was found in Privoxy before 3.0.29 in the show-status CGI handler when no action files are configured.	2021-05-25	5	CVE-2021-20209 MISC MISC MISC
putty -- putty	PuTTY before 0.75 on Windows allows remote servers to cause a denial of service (Windows GUI hang) by telling the PuTTY window to change its title repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls. NOTE: the same attack methodology may affect some OS-level GUIs on Linux or other platforms for similar reasons.	2021-05-21	5	CVE-2021-33500 MISC MISC MISC
redhat -- ansible	A flaw was found in OpenLDAP. This flaw allows an attacker who can send a malicious packet to be processed by OpenLDAP's slapd server, to trigger an assertion failure. The highest threat from this vulnerability is to system availability.	2021-05-24	5	CVE-2020-20178 MISC
solokeys -- solo_firmware	The flash read-out protection (RDP) level is not enforced during the device initialization phase of the SoloKeys Solo 4.0.0 & Somu and the Nitrokey FIDO2 token. This allows an adversary to downgrade the RDP level and access secrets such as private ECC keys from SRAM via the debug interface.	2021-05-21	4.6	CVE-2020-27208 MISC MISC MISC MISC MISC MISC
synology -- diskstation_manager	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Synology DiskStation Manager. Authentication is not required to exploit this vulnerablity. The specific flaw exists within the processing of DSI structures in Netatalk. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12326.	2021-05-21	5.8	CVE-2021-31439 MISC MISC
targetfirst -- watcheezy	The Target First WordPress Plugin v2.0, also previously known as Watcheezy, suffers from a critical unauthenticated stored XSS vulnerability. An attacker could change the licence key value through a POST on any URL	2021-05-24	4.3	CVE-2021-24305 MISC CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with the 'weeWzKey' parameter that will be save as the 'weeID option and is not sanitized.			
telop01_project -- telop01	Reflected cross-site scripting vulnerability in the admin page of [Telop01] free edition ver1.0.1 and earlier allows a remote attacker to inject an arbitrary script via unspecified vectors.	2021-05-24	4.3	CVE-2021-20724 MISC MISC
trailing-slash_project -- trailing-slash	The package trailing-slash before 2.0.1 are vulnerable to Open Redirect via the use of trailing double slashes in the URL when accessing the vulnerable endpoint (such as https://example.com//attacker.example/). The vulnerable code is in index.js::createTrailing(), as the web server uses relative URLs instead of absolute URLs.	2021-05-24	5.8	CVE-2021-23387 MISC MISC MISC
typora -- typora	Cross Site Scripting (XSS) in Typora v0.9.65 and earlier allows remote attackers to execute arbitrary code by injecting commands during block rendering of a mathematical formula.	2021-05-26	4.3	CVE-2020-18221 MISC
wago -- 750-823_firmware	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime.	2021-05-24	5	CVE-2021-21000 CONFIRM
wago -- 750-823_firmware	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges.	2021-05-24	4	CVE-2021-21001 CONFIRM
webfairy -- mediat	An issue was discovered in Mediat 1.4.1. There is a Reflected XSS vulnerability which allows remote attackers to inject arbitrary web script or HTML without authentication via the 'return' parameter in login.php.	2021-05-24	4.3	CVE-2021-30083 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function ShiftBytes. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	6.4	CVE-2018-25013 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function ApplyFilter. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	6.4	CVE-2018-25010 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function ChunkVerifyAndAssign. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	6.4	CVE-2020-36330 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. When reading a file libwebp allocates an excessive amount of memory. The highest threat from this vulnerability is to the service availability.	2021-05-21	5	CVE-2020-36332 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function ChunkAssignData. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	6.4	CVE-2020-36331 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function WebPMuxCreateInternal. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	6.4	CVE-2018-25012 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function WebPMuxCreateInternal. The highest threat from this vulnerability is to data confidentiality and to the service availability.	2021-05-21	6.4	CVE-2018-25009 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zephyrproject -- zephyr	Missing Size Checks in Bluetooth HCI over SPI. Zephyr versions >= v1.14.2, >= v2.2.0 contain Improper Handling of Length Parameter Inconsistency (CWE-130). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-hg2w-62p6-g67c	2021-05-25	5.8	CVE-2020-10065 MISC
zephyrproject -- zephyr	Type Confusion in 802154 ACK Frames Handling. Zephyr versions >= v2.4.0 contain NULL Pointer Dereference (CWE-476). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-27r3-rxch-2hm7	2021-05-25	5	CVE-2021-3320 MISC
zephyrproject -- zephyr	Integer Overflow in memory allocating functions. Zephyr versions >= 1.14.2, >= 2.4.0 contain Integer Overflow or Wraparound (CWE-190). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-94vp-8gc2-rm45	2021-05-25	4.6	CVE-2020-13603 MISC
zephyrproject -- zephyr	Improper Handling of Insufficient Permissions or Privileges in zephyr. Zephyr versions >= v1.14.2, >= v2.2.0 contain Improper Handling of Insufficient Permissions or Privileges (CWE-280). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-vf79-hqwm-w4xc	2021-05-25	4.6	CVE-2020-10072 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autoptimize -- autoptimize	The Autoptimize WordPress plugin before 2.8.4 was missing proper escaping and sanitisation in some of its settings, allowing high privilege users to set XSS payloads in them, leading to stored Cross-Site Scripting issues	2021-05-24	3.5	CVE-2021-24332 CONFIRM MISC
bluemedicinelabs -- hotjar_connecticator	The Hotjar Connecticator WordPress plugin through 1.1.1 is vulnerable to Stored Cross-Site Scripting (XSS) in the 'hotjar script' textarea. The request did include a CSRF nonce that was properly verified by the server and this vulnerability could only be exploited by administrator users.	2021-05-24	3.5	CVE-2021-24301 CONFIRM
centreon -- centreon	Centreon version 20.10.2 is affected by a cross-site scripting (XSS) vulnerability. The dep_description (Dependency Description) and dep_name (Dependency Name) parameters are vulnerable to stored XSS. A user has to log in and go to the Configuration > Notifications > Hosts page.	2021-05-26	3.5	CVE-2021-27676 MISC MISC
cisco -- evolved_programmable_network_manager	A vulnerability in the restricted shell of Cisco Evolved Programmable Network (EPN) Manager, Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to identify directories and write arbitrary files to the file system. This vulnerability is due to improper validation of parameters that are sent to a CLI command within the restricted shell. An attacker could exploit	2021-05-22	3.6	CVE-2021-1306 CISCO

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	this vulnerability by logging in to the device and issuing certain CLI commands. A successful exploit could allow the attacker to identify file directories on the affected device and write arbitrary files to the file system on the affected device. To exploit this vulnerability, the attacker must be an authenticated shell user.			
gowebsolutions -- wp_customer_reviews	The WP Customer Reviews WordPress plugin before 3.5.6 did not sanitise some of its settings, allowing high privilege users such as administrators to set XSS payloads in them which will then be triggered in pages where reviews are enabled	2021-05-24	3.5	CVE-2021-24296 CONFIRM
ibm -- security_guardium	IBM Security Guardium 11.2 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 195770.	2021-05-24	2.1	CVE-2021-20389 CONFIRM XF
keystonejs -- keystone-5	Keystone 5 is an open source CMS platform to build Node.js applications. This security advisory relates to a newly discovered capability in our query infrastructure to directly or indirectly expose the values of private fields, bypassing the configured access control. This is an access control related oracle attack in that the attack method guides an attacker during their attempt to reveal information they do not have access to. The complexity of completing the attack is limited by some length-dependent behaviors and the fidelity of the exposed information. Under some circumstances, field values or field value meta data can be determined, despite the field or list having `read` access control configured. If you use private fields or lists, you may be impacted. No patches exist at this time. There are no workarounds at this time	2021-05-24	3.5	CVE-2021-32624 CONFIRM
lifterlms -- lifterlms	The 'State' field of the Edit profile page of the LMS by LifterLMS – Online Course, Membership & Learning Management System Plugin for WordPress plugin before 4.21.1 is not properly sanitised when output in the About section of the profile page, leading to a stored Cross-Site Scripting issue. This could allow low privilege users (such as students) to elevate their privilege via an XSS attack when an admin will view their profile.	2021-05-24	3.5	CVE-2021-24308 MISC CONFIRM MISC
neox -- hana_flv_player	The Hana Flv Player WordPress plugin through 3.1.3 is vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) vulnerability within the 'Default Skin' field.	2021-05-24	3.5	CVE-2021-24302 CONFIRM
phpmywind -- phpmywind	Cross Site Scripting (XSS) in PHPMyWind v5.5 allows remote attackers to execute arbitrary code by injecting scripts into the parameter "$cfg_switchshow" of component " /admin/web_config.php".	2021-05-27	3.5	CVE-2020-18230 MISC
phpmywind -- phpmywind	Cross Site Scripting (XSS) in PHPMyWind v5.5 allows remote attackers to execute arbitrary code by injecting scripts into the parameter "$cfg_copyright" of component " /admin/web_config.php".	2021-05-27	3.5	CVE-2020-18229 MISC
plone -- plone	Plone through 5.2.4 allows stored XSS attacks (by a Contributor) by uploading an SVG or HTML document.	2021-05-21	3.5	CVE-2021-33512 MISC MLIST
plone -- plone	Plone through 5.2.4 allows XSS via the inline_diff methods in Products.CMFDiffTool.	2021-05-21	3.5	CVE-2021-33513 MISC MLIST

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
plone -- plone	Plone through 5.2.4 allows XSS via a full name that is mishandled during rendering of the ownership tab of a content item.	2021-05-21	3.5	CVE-2021-33508 MISC MLIST
postbird_project -- postbird	Postbird 0.8.4 allows stored XSS via the onerror attribute of an IMG element in any PostgreSQL database table. This can result in reading local files via vectors involving XMLHttpRequest and open of a file:/// URL, or discovering PostgreSQL passwords via vectors involving Window.localStorage and savedConnections.	2021-05-25	3.5	CVE-2021-33570 MISC MISC MISC MISC MISC
shopizer -- shopizer	A stored cross-site scripting (XSS) vulnerability in Shopizer before 2.17.0 allows remote attackers to inject arbitrary web script or HTML via customer_name in various forms of store administration. It is saved in the database. The code is executed for any user of store administration when information is fetched from the backend, e.g., in admin/customers/list.html.	2021-05-24	3.5	CVE-2021-33561 MISC MISC MISC
shopizer -- shopizer	A reflected cross-site scripting (XSS) vulnerability in Shopizer before 2.17.0 allows remote attackers to inject arbitrary web script or HTML via the ref parameter to a page about an arbitrary product, e.g., a product/insert-product-name-here.html/ref= URL.	2021-05-24	3.5	CVE-2021-33562 MISC MISC MISC
zephyrproject -- zephyr	Incorrect Error Handling in Bluetooth HCI core. Zephyr versions >= v1.14.2, >= v2.2.0 contain NULL Pointer Dereference (CWE-476). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-gc66-xfrc-24qr	2021-05-25	3.3	CVE-2020-10066 MISC
zephyrproject -- zephyr	Zephyr Bluetooth unchecked packet data results in denial of service. Zephyr versions >= v1.14.2, >= v2.2.0 contain Improper Handling of Parameters (CWE-233). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-f6vh-7v4x-8fjp	2021-05-25	3.3	CVE-2020-10069 MISC
zephyrproject -- zephyr	Remote Denial of Service in LwM2M do_write_op_tlv. Zephyr versions >= 1.14.2, >= 2.2.0 contain Improper Input Validation (CWE-20), Loop with Unreachable Exit Condition ('Infinite Loop') (CWE-835). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-g9mg-fj58-6fqh	2021-05-25	2.1	CVE-2020-13602 MISC