BULLETIN (SB22-031)

VULNERABILITY SUMMARY FOR THE WEEK OF

24TH JANUARY, 2022

Bulletin (SB22-031)
Vulnerability Summary for the Week of January 24, 2022

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
xorux -- lpar2rrd	A shell command injection in the HW Events SNMP community in XoruX LPAR2RRD and STOR2RRD before 7.30 allows authenticated remote attackers to execute arbitrary shell commands as the user running the service.	2021-11-08	9	CVE-2021-42372
apache -- shenyu	Groovy Code Injection & SpEL Injection which lead to Remote Code Execution. This issue affected Apache ShenYu 2.4.0 and 2.4.1.	2022-01-25	7.5	CVE-2021-45029 MLIST MLIST
asus -- vc65-c1_firmware	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service.	2022-01-21	7.2	CVE-2022-21933
budget_and_expense_tracker_system_project -- budget_and_expense_tracker_system	SQL injection vulnerability in Sourcecodester Budget and Expense Tracker System v1 by oretnom23, allows attackers to execute arbitrary SQL commands via the username field.	2022-01-21	7.5	CVE-2021-40247
cached-path-relative_project -- cached-path-relative	The package cached-path-relative before 1.1.0 are vulnerable to Prototype Pollution via the cache variable that is set as {} instead of Object.create(null) in the cachedPathRelative function, which allows access to the parent prototype properties when the object is used to create the cached relative path. When using the origin path as __proto__, the attribute of the object is accessed instead of a path. **Note:** This vulnerability derives from an incomplete fix in https://security.snyk.io/vuln/SNYK-JS-CACHEDPATHRELATIVE-72573	2022-01-21	7.5	CVE-2021-23518
courier_management_system_project -- courier_management_system	An SQL Injection vulnerability exists in Sourceodester Courier Management System 1.0 via the email parameter in /cms/ajax.php app.	2022-01-21	10	CVE-2021-46198
dell -- emc_appsync	Dell EMC AppSync versions 3.9 to 4.3 contain an Improper Restriction of Excessive Authentication Attempts Vulnerability that can be exploited from UI and CLI. An adjacent unauthenticated attacker could potentially exploit this vulnerability, leading to password brute-forcing. Account takeover is possible if weak passwords are used by users.	2022-01-21	7.5	CVE-2022-22553
dell -- emc_unity_operating_environment	Dell EMC Unity, Dell EMC UnityVSA and Dell EMC Unity XT versions prior to 5.1.2.0.5.007 contain an operating system (OS) command injection Vulnerability. A locally authenticated user with high privileges may potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the Unity underlying OS, with the privileges of the vulnerable application. Exploitation may lead to an elevation of privilege.	2022-01-24	7.2	CVE-2021-43589
employee_and_visitor_gate_pass_logging_system_project -- employee_and_visitor_gate_pass_logging_system	An SQL Injection vulnerability exists in Sourcecodester Employee and Visitor Gate Pass Logging System 1.0 via the username parameter.	2022-01-21	10	CVE-2021-46309
europa -- technical_specifications_for_digital_covid_certificates	The EU Technical Specifications for Digital COVID Certificates before 1.1 mishandle certificate governance. A non-production public key certificate could have been used in production.	2022-01-21	7.5	CVE-2021-40855
exiftool_project -- exiftool	lib/Image/ExifTool.pm in ExifTool before 12.38 mishandles a $file =~ /\|$/ check.	2022-01-25	7.5	CVE-2022-23935
forestblog_project -- forestblog	In ForestBlog, as of 2021-12-28, File upload can bypass verification.	2022-01-25	7.5	CVE-2021-46033
freecadweb -- freecad	Improper sanitization in the invocation of ODA File Converter from FreeCAD 0.19 allows an attacker to inject OS commands via a crafted filename.	2022-01-25	7.6	CVE-2021-45844
fresenius-kabi -- agilia_connect_firmware	The web application on Agilia Link+ version 3.0 implements authentication and session management mechanisms exclusively on the client-side and does not protect authentication attributes sufficiently.	2022-01-21	7.5	CVE-2021-23196
fresenius-kabi -- agilia_partner_maintenance_software	Requests may be used to interrupt the normal operation of the device. When exploited, Fresenius Kabi Agilia Link+ version 3.0 must be rebooted via a hard reset triggered by pressing a button on the rack system.	2022-01-21	7.8	CVE-2021-23236

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fresenius-kabi -- agilia_partner_maintenance_software	Fresenius Kabi Vigilant Software Suite (Mastermed Dashboard) version 2.0.1.3 allows user input to be validated on the client side without authentication by the server. The server should not rely on the correctness of the data because users might not support or block JavaScript or intentionally bypass the client-side checks. An attacker with knowledge of the service user could circumvent the client-side control and login with service privileges.	2022-01-21	7.5	CVE-2021-43355
fresenius-kabi -- agilia_partner_maintenance_software	Sensitive endpoints in Fresenius Kabi Agilia Link+ v3.0 and prior can be accessed without any authentication information such as the session cookie. An attacker can send requests to sensitive endpoints as an unauthenticated user to perform critical actions or modify critical configuration parameters.	2022-01-21	7.5	CVE-2021-23233
hms_project -- hms	HMS v1.0 was discovered to contain a SQL injection vulnerability via patientlogin.php.	2022-01-21	7.5	CVE-2022-23366
hms_project -- hms	HMS v1.0 was discovered to contain a SQL injection vulnerability via adminlogin.php.	2022-01-21	7.5	CVE-2022-23364
hms_project -- hms	HMS v1.0 was discovered to contain a SQL injection vulnerability via doctorlogin.php.	2022-01-21	7.5	CVE-2022-23365
ibm -- cognos_controller	IBM Cognos Controller 10.4.0, 10.4.1, and 10.4.2 could allow a remote attacker to bypass security restrictions, caused by improper validation of authentication cookies. IBM X-Force ID: 190847.	2022-01-21	7.5	CVE-2020-4879 XF
ibm -- cognos_controller	IBM Cognos Controller 10.4.0, 10.4.1, and 10.4.2 could be vulnerable to unauthorized modifications by using public fields in public classes. IBM X-Force ID: 190843.	2022-01-21	7.5	CVE-2020-4877 XF
iconics -- analytix	Incomplete List of Disallowed Inputs vulnerability in Mitsubishi Electric MC Works64 versions 4.00A (10.95.201.23) to 4.04E (10.95.210.01), ICONICS GENESIS64 versions 10.95.3 to 10.97, ICONICS Hyper Historian versions 10.95.3 to 10.97, ICONICS AnalytiX versions 10.95.3 to 10.97 and ICONICS MobileHMI versions 10.95.3 to 10.97 allows a remote unauthenticated attacker to bypass the authentication of MC Works64, GENESIS64, Hyper Historian, AnalytiX and MobileHMI, and gain unauthorized access to the products, by sending specially crafted WebSocket packets to FrameWorX server, one of the functions of the products.	2022-01-21	7.5	CVE-2022-23128
iresturant_project -- iresturant	MartDevelopers iResturant 1.0 is vulnerable to SQL Injection. SQL Injection occurs because the email and phone parameter values are added to the SQL query without any verification at the time of membership registration.	2022-01-25	7.5	CVE-2021-45802
jeecg -- jeecg_boot	In JeecgBoot 3.0, there is a SQL injection vulnerability that can operate the database with root privileges.	2022-01-25	10	CVE-2021-46089
libexpat_project -- libexpat	Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES.	2022-01-24	7.5	CVE-2022-23852
librecad -- librecad	A buffer overflow vulnerability in CDataMoji of the jwwlib component of LibreCAD 2.2.0-rc3 and older allows an attacker to achieve Remote Code Execution using a crafted JWW document.	2022-01-25	9.3	CVE-2021-45341
loguru_project -- loguru	Code Injection in PyPi loguru prior to and including 0.5.3.	2022-01-21	7.5	CVE-2022-0329
mediatek -- linkit_software_development_kit	In MediaTek LinkIt SDK before 4.6.1, there is a possible memory corruption due to an integer overflow during mishandled memory allocation by pvPortCalloc and pvPortRealloc.	2022-01-24	7.5	CVE-2021-30636
mingsoft -- mcms	MCMS v5.2.4 was discovered to have an arbitrary file upload vulnerability in the New Template module, which allows attackers to execute arbitrary code via a crafted ZIP file.	2022-01-21	7.5	CVE-2022-22929
mingsoft -- mcms	MCMS v5.2.4 was discovered to have a hardcoded shiro-key, allowing attackers to exploit the key and execute arbitrary code.	2022-01-21	7.5	CVE-2022-22928
mingsoft -- mcms	MCMS v5.2.4 was discovered to contain a SQL injection vulnerability via /ms/mdiy/model/importJson.do.	2022-01-21	7.5	CVE-2022-23314
mingsoft -- mcms	A remote code execution (RCE) vulnerability in the Template Management function of MCMS v5.2.4 allows attackers to execute arbitrary code via a crafted payload.	2022-01-21	7.5	CVE-2022-22930
mingsoft -- mcms	MCMS v5.2.4 was discovered to contain an arbitrary file upload vulnerability via the component /ms/template/writeFileContent.do.	2022-01-21	7.5	CVE-2022-23315
online_banking_system_project -- online_banking_system	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via index.php.	2022-01-21	7.5	CVE-2022-23363

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
online_learning_system_project -- online_learning_system	SQL injection vulnerability in Login.php in sourcecodester Online Learning System v2 by oretnom23, allows attackers to execute arbitrary SQL commands via the faculty_id parameter.	2022-01-24	7.5	CVE-2021-40596
online_leave_management_system_project -- online_leave_management_system	SQL injection vulnerability in Sourcecodester Online Leave Management System v1 by oretnom23, allows attackers to execute arbitrary SQL commands via the username parameter to /leave_system/classes/Login.php.	2022-01-21	7.5	CVE-2021-40595
online_payment_hub_project -- online_payment_hub	SQL injection vulnerability in Login.php in Sourcecodester Online Payment Hub v1 by oretnom23, allows attackers to execute arbitrary SQL commands via the username parameter.	2022-01-24	7.5	CVE-2021-43420
online_project_time_management_system_project -- online_project_time_management_system	An SQL Injection vulnerabilty exists in Sourcecodester Online Project Time Management System 1.0 via the pid parameter in the load_file function.	2022-01-24	7.5	CVE-2021-46451
online_railway_reservation_system_project -- online_railway_reservation_system	An SQL Injection vulnerability exists in Sourcecodester Online Railway Reservation Sysytem 1.0 via the sid parameter.	2022-01-21	10	CVE-2021-46308
online_resort_management_system_project -- online_resort_management_system	An SQL Injection vulnerability exists in Sourcecodester Online Resort Management System 1.0 via the id parameterv in /orms/ node.	2022-01-21	10	CVE-2021-46201
projectworlds -- online-shopping-webvsite-in-php	Projectworlds online-shopping-webvsite-in-php 1.0 suffers from a SQL Injection vulnerability via the "id" parameter in cart_add.php, No login is required.	2022-01-23	7.5	CVE-2021-46024
projectworlds -- online_examination_system	An SQL Injection vulnerability exists in Projectworlds Online Examination System 1.0 via the eid parameter in account.php.	2022-01-21	10	CVE-2021-46307
purchase_order_management_system_project -- purchase_order_management_system	SQL injection vulnerability in Login.php in Sourcecodester Purchase Order Management System v1 by oretnom23, allows attackers to execute arbitrary SQL commands via the username parameter.	2022-01-24	7.5	CVE-2021-40908
quickbox -- quickbox	In QuickBox Pro v2.5.8 and below, the config.php file has a variable which takes a GET parameter value and parses it into a shell_exec(''); function without properly sanitizing any shell arguments, therefore remote code execution is possible. Additionally, as the media server is running as root by default attackers can use the sudo command within this shell_exec(''); function, which allows for privilege escalation by means of RCE.	2022-01-24	9	CVE-2021-44981
saviynt -- enterprise_identity_cloud	An issue was discovered in Saviynt Enterprise Identity Cloud (EIC) 5.5 SP2.x. An authentication bypass in ECM/maintenance/forgotpasswordstep1 allows an unauthenticated user to reset passwords and login as any local account.	2022-01-24	7.5	CVE-2022-23855
simple_membership_system_using_php_and_ajax_project -- simple_membership_system_using_php_and_ajax	SQL injection vulnerability in Sourcecodester Simple Membership System v1 by oretnom23, allows attackers to execute arbitrary SQL commands via the username and password parameters.	2022-01-24	7.5	CVE-2021-41472
simple_music_cloud_community_system_project -- simple_music_cloud_community_system	An SQL Injection vulnerability exists in Sourcecodester Simple Music Clour Community System 1.0 via the email parameter in /music/ajax.php.	2022-01-21	10	CVE-2021-46200

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
south_gate_inn_online_reservation_system_project -- south_gate_inn_online_reservation_system	SQL injection vulnerability in Sourcecodester South Gate Inn Online Reservation System v1 by oretnom23, allows attackers to execute arbitrary SQL commands via the email and Password parameters.	2022-01-24	7.5	CVE-2021-41471
starwindsoftware -- command_center	In StarWind Command Center before V2 build 6021, an authenticated read-only user can elevate privileges to administrator through the REST API.	2022-01-24	9	CVE-2022-23858
storage_unit_rental_management_system_project -- storage_unit_rental_management_system	SQL injection vulnerability in Sourcecodester Storage Unit Rental Management System v1 by oretnom23, allows attackers to execute arbitrary SQL commands via the username parameter to /storage/classes/Login.php.	2022-01-24	7.5	CVE-2021-40907
telosalliance -- z\/ip_one_firmware	A directory traversal vulnerability on Telos Z/IP One devices through 4.0.0r grants an unauthenticated individual root level access to the device's file system. This can be used to identify configuration settings, password hashes for built-in accounts, and the cleartext password for remote configuration of the device through the WebUI.	2022-01-24	10	CVE-2020-17383
teslamate_project -- teslamate	TeslaMate before 1.25.1 (when using the default Docker configuration) allows attackers to open doors of Tesla vehicles, start Keyless Driving, and interfere with vehicle operation en route. This occurs because an attacker can leverage Grafana login access to obtain a token for Tesla API calls.	2022-01-24	7.5	CVE-2022-23126
tp-link -- archer_c90_firmware	This vulnerability allows remote attackers to execute arbitrary code on affected installations of TP-Link Archer C90 1.0.6 Build 20200114 rel.73164(5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of DNS responses. A crafted DNS message can trigger an overflow of a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-14655.	2022-01-21	10	CVE-2021-35003
tp-link -- tl-wa1201_firmware	This vulnerability allows remote attackers to execute arbitrary code on affected installations of TP-Link TL-WA1201 1.0.1 Build 20200709 rel.66244(5553) wireless access points. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of DNS responses. A crafted DNS message can trigger an overflow of a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-14656.	2022-01-21	10	CVE-2021-35004
try_my_recipe_project -- try_my_recipe	SQL injection in Sourcecodester Try My Recipe (Recipe Sharing Website - CMS) 1.0 by oretnom23, allows attackers to execute arbitrary code via the rid parameter to the view_recipe page.	2022-01-24	7.5	CVE-2021-41928
usbview_project -- usbview	USBView 2.1 before 2.2 allows some local users (e.g., ones logged in via SSH) to execute arbitrary code as root because certain Polkit settings (e.g., allow_any=yes) for pkexec disable the authentication requirement. Code execution can, for example, use the --gtk-module option. This affects Ubuntu, Debian, and Gentoo.	2022-01-21	7.2	CVE-2022-23220 DEBIAN MLIST
vim -- vim	Heap-based Buffer Overflow in vim/vim prior to 8.2.	2022-01-21	7.5	CVE-2022-0318
wedevs -- wp_user_frontend	The WP User Frontend WordPress plugin before 3.5.26 does not validate and escape the status parameter before using it in a SQL statement in the Subscribers dashboard, leading to an SQL injection. Due to the lack of sanitisation and escaping, this could also lead to Reflected Cross-Site Scripting	2022-01-24	7.5	CVE-2021-25076
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-45062
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-44707
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user.	2022-01-14	9.3	CVE-2021-45061

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-45060
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-44711
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-44710
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a heap overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-44708
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a heap overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-44709
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-44706
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-44705
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-44704
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a stack buffer overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-44703
adobe -- bridge	Adobe Bridge version 11.1.2 (and earlier) and version 12.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	9.3	CVE-2021-44743
arm -- bifrost_gpu_kernel_driver	Arm Mali GPU Kernel Driver (Midgard r26p0 through r30p0, Bifrost r0p0 through r34p0, and Valhall r19p0 through r34p0) allows a non-privileged user to achieve write access to read-only memory, and possibly obtain root privileges, corrupt memory, and modify the memory of other processes.	2022-01-14	7.2	CVE-2021-44828
dolibarr -- dolibarr	dolibarr is vulnerable to Improper Neutralization of Special Elements used in an SQL Command	2022-01-14	7.5	CVE-2022-0224
gnu -- glibc	The deprecated compatibility function clnt_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its hostname argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.	2022-01-14	7.5	CVE-2022-23219
gnu -- glibc	The deprecated compatibility function svcunix_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its path argument on the stack	2022-01-14	7.5	CVE-2022-23218

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.			
google -- android	In fs/eventpoll.c, there is a possible use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-204450605References: Upstream kernel	2022-01-14	7.2	CVE-2021-39634
google -- android	In sendLegacyVoicemailNotification of LegacyModeSmsHandler.java, there is a possible permissions bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-185126549	2022-01-14	7.2	CVE-2021-39627
google -- android	In executeRequest of OverlayManagerService.java, there is a possible way to control fabricated overlays from adb shell due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-202768292	2022-01-14	7.2	CVE-2021-39630
google -- android	In inotify_cb of events.cpp, 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.Product: AndroidVersions: Android-11 Android-12Android ID: A-202159709	2022-01-14	7.2	CVE-2021-39632
google -- android	Hacker one bug ID: 1343975Product: AndroidVersions: Android SoCAndroid ID: A-204256722	2022-01-14	10	CVE-2021-1049
google -- android	In <TBD> of <TBD>, there is a possible bypass of Factory Reset Protection due to <TBD>. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-171742549References: N/A	2022-01-14	7.2	CVE-2021-39678
google -- android	In mgm_alloc_page of memory_group_manager.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.Product: AndroidVersions: Android kernelAndroid ID: A-201677538References: N/A	2022-01-14	7.2	CVE-2021-39682
google -- android	In copy_from_mbox of sss_ice_util.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-202003354References: N/A	2022-01-14	7.2	CVE-2021-39683
google -- android	In target_init of gs101/abl/target/slider/target.c, there is a possible allocation of RWX memory 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.Product: AndroidVersions: Android kernelAndroid ID: A-203250788References: N/A	2022-01-14	7.2	CVE-2021-39684
google -- android	In onAttach of ConnectedDeviceDashboardFragment.java, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-194695497	2022-01-14	7.2	CVE-2021-39626
google -- android	In sendLegacyVoicemailNotification of LegacyModeSmsHandler.java, there is a possible permissions bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-185126319	2022-01-14	7.2	CVE-2021-39621
ibm -- filenet_content_manager	IBM FileNet Content Manager 5.5.4, 5.5.6, and 5.5.7 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 212346.	2022-01-17	9	CVE-2021-38965 XF
imperva -- web_application_firewall	Imperva Web Application Firewall (WAF) before 2021-12-23 allows remote unauthenticated attackers to use "Content-Encoding: gzip" to evade WAF security controls and send malicious HTTP POST requests to web servers behind the WAF.	2022-01-14	7.5	CVE-2021-45468
le-yan_dental_management_system_project -- le-yan_dental_management_system	The Le-yan dental management system contains an SQL-injection vulnerability. An unauthenticated remote attacker can inject SQL commands into the input field of the login page to acquire administrator's privilege and perform arbitrary operations on the system or disrupt service.	2022-01-14	10	CVE-2022-22055

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
le-yan_dental_management_system_project -- le-yan_dental_management_system	The Le-yan dental management system contains a hard-coded credentials vulnerability in the web page source code, which allows an unauthenticated remote attacker to acquire administrator's privilege and control the system or disrupt service.	2022-01-14	10	CVE-2022-22056
linux -- linux_kernel	kernel/bpf/verifier.c in the Linux kernel through 5.15.14 allows local users to gain privileges because of the availability of pointer arithmetic via certain *_OR_NULL pointer types.	2022-01-14	7.2	CVE-2022-23222 MLIST MLIST DEBIAN
mitsubishielectric -- fx3u-enet_firmware	Lack of administrator control over security vulnerability in MELSEC-F series FX3U-ENET Firmware version 1.14 and prior, FX3U-ENET-L Firmware version 1.14 and prior and FX3U-ENET-P502 Firmware version 1.14 and prior allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition in communication function of the product or other unspecified effects by sending specially crafted packets to an unnecessary opening of TCP port. Control by MELSEC-F series PLC is not affected by this vulnerability, but system reset is required for recovery.	2022-01-14	7.8	CVE-2021-20612
mitsubishielectric -- fx3u-enet_firmware	Improper initialization vulnerability in MELSEC-F series FX3U-ENET Firmware version 1.16 and prior, FX3U-ENET-L Firmware version 1.16 and prior and FX3U-ENET-P502 Firmware version 1.16 and prior allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition in communication function of the product by sending specially crafted packets. Control by MELSEC-F series PLC is not affected by this vulnerability, but system reset is required for recovery.	2022-01-14	7.8	CVE-2021-20613
nuuo -- nvrmini2_firmware	NUUO NVRmini2 through 3.11 allows an unauthenticated attacker to upload an encrypted TAR archive, which can be abused to add arbitrary users because of the lack of handle_import_user.php authentication. When combined with another flaw (CVE-2011-5325), it is possible to overwrite arbitrary files under the web root and achieve code execution as root.	2022-01-14	10	CVE-2022-23227
oracle -- access_manager	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: OpenSSO Agent). Supported versions that are affected are 11.1.2.3.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in takeover of Oracle Access Manager. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2022-01-19	7.5	CVE-2021-35587
oracle -- communications_billing_and_revenue_management	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in Oracle Communications Billing and Revenue Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2022-01-19	7.5	CVE-2022-21275
oracle -- installed_base	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: Instance Main). Supported versions that are affected are 12.2.3-12.2.11. 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 ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Installed Base. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2022-01-19	7.8	CVE-2022-21251
owncloud -- files_antivirus	The files_antivirus component before 1.0.0 for ownCloud allows OS Command Injection via the administration settings.	2022-01-15	9	CVE-2021-33827
qnap -- qvr_elite	A stack buffer overflow vulnerability has been reported to affect QNAP device running QVR Elite, QVR Pro, QVR Guard. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QVR Elite, QVR Pro, QVR Guard: QuTS hero h5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QuTS hero h4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 5.0.0: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Elite 2.1.4.0 (2021/12/06) and later QTS 4.5.4: QVR Pro 2.1.3.0 (2021/12/06) and later	2022-01-14	7.5	CVE-2021-38692

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	QTS 5.0.0: QVR Pro 2.1.3.0 (2021/12/06) and later QTS 4.5.4: QVR Guard 2.1.3.0 (2021/12/06) and later QTS 5.0.0: QVR Guard 2.1.3.0 (2021/12/06) and later			
sap -- s\/4hana	The F0743 Create Single Payment application of SAP S/4HANA - versions 100, 101, 102, 103, 104, 105, 106, does not check uploaded or downloaded files. This allows an attacker with basic user rights to inject dangerous content or malicious code which could result in critical information being modified or completely compromise the availability of the application.	2022-01-14	7.5	CVE-2022-22530
stanford -- corenlp	corenlp is vulnerable to Improper Restriction of XML External Entity Reference	2022-01-17	7.5	CVE-2022-0239
agoric -- realms-shim	All versions of package realms-shim are vulnerable to Sandbox Bypass via a Prototype Pollution attack vector.	2022-01-10	7.5	CVE-2021-23543
agoric -- realms-shim	All versions of package realms-shim are vulnerable to Sandbox Bypass via a Prototype Pollution attack vector.	2022-01-10	7.5	CVE-2021-23594
checkpoint -- endpoint_security	Users have access to the directory where the installation repair occurs. Since the MS Installer allows regular users to run the repair, an attacker can initiate the installation repair and place a specially crafted EXE in the repair folder which runs with the Check Point Remote Access Client privileges.	2022-01-10	7.2	CVE-2021-30360
chshcms -- cscms	cscms v4.1 allows for SQL injection via the "page_del" function.	2022-01-11	7.5	CVE-2020-28103
chshcms -- cscms	cscms v4.1 allows for SQL injection via the "js_del" function.	2022-01-11	7.5	CVE-2020-28102
cisco -- unified_contact_center_express	A vulnerability in the web-based management interface of Cisco Unified Contact Center Management Portal (Unified CCMP) and Cisco Unified Contact Center Domain Manager (Unified CCDM) could allow an authenticated, remote attacker to elevate their privileges to Administrator. This vulnerability is due to the lack of server-side validation of user permissions. An attacker could exploit this vulnerability by submitting a crafted HTTP request to a vulnerable system. A successful exploit could allow the attacker to create Administrator accounts. With these accounts, the attacker could access and modify telephony and user resources across all the Unified platforms that are associated to the vulnerable Cisco Unified CCMP. To successfully exploit this vulnerability, an attacker would need valid Advanced User credentials.	2022-01-14	8.5	CVE-2022-20658 CISCO
eggjs -- extend2	The package extend2 before 1.0.1 are vulnerable to Prototype Pollution via the extend function due to unsafe recursive merge.	2022-01-10	7.5	CVE-2021-23568
fanuc -- r-30ia_firmware	The FANUC R-30iA and R-30iB series controllers are vulnerable to an out-of-bounds write, which may allow an attacker to remotely execute arbitrary code. INIT START/restore from backup required.	2022-01-10	10	CVE-2021-32998
fanuc -- r-30ia_firmware	The FANUC R-30iA and R-30iB series controllers are vulnerable to integer coercion errors, which cause the device to crash. A restart is required.	2022-01-10	7.8	CVE-2021-32996
google -- android	In ipcSetDataReference of Parcel.cpp, there is a possible way to corrupt memory 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.Product: AndroidVersions: Android-11 Android-12Android ID: A-203847542	2022-01-14	7.2	CVE-2021-39620
google -- android	In GBoard, there is a possible way to bypass Factory Reset Protection due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-192663648	2022-01-14	7.2	CVE-2021-39622
google -- android	In jit_memory_region.cc, there is a possible bypass of memory restrictions due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-200284993	2022-01-14	7.2	CVE-2021-0959
google -- android	In multiple methods of EuiccNotificationManager.java, there is a possible way to install existing packages without user consent due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-196855999	2022-01-14	7.2	CVE-2021-39618
google -- android	In setLaunchIntent of BluetoothDevicePickerPreferenceController.java, there is a possible way to invoke an arbitrary broadcast receiver due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-12Android ID: A-195668284	2022-01-14	7.2	CVE-2021-1035
google -- android	In doRead of SimpleDecodingSource.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote escalation of privilege	2022-01-14	10	CVE-2021-39623

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-194105348			
huawei -- emui	There is an Integer overflow vulnerability with ACPU in smartphones. Successful exploitation of this vulnerability may cause out-of-bounds access.	2022-01-10	7.5	CVE-2021-39993
huawei -- harmonyos	There is Vulnerability of APIs being concurrently called for multiple times in HwConnectivityExService a in smartphones. Successful exploitation of this vulnerability may cause the system to crash and restart.	2022-01-10	7.8	CVE-2021-39998
huawei -- harmonyos	The bone voice ID trusted application (TA) has a heap overflow vulnerability. Successful exploitation of this vulnerability may result in malicious code execution.	2022-01-10	7.5	CVE-2021-40010
huawei -- harmonyos	There is a Heap-based buffer overflow vulnerability with the NFC module in smartphones. Successful exploitation of this vulnerability may cause memory overflow.	2022-01-10	7.5	CVE-2021-39996
laundry_booking_management_system_project -- laundry_booking_management_system	Laundry Booking Management System 1.0 (Latest) and previous versions are affected by a remote code execution (RCE) vulnerability in profile.php through the "image" parameter that can execute a webshell payload.	2022-01-10	7.5	CVE-2021-45003
libexpat_project -- libexpat	defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	2022-01-10	7.5	CVE-2022-22824
libexpat_project -- libexpat	build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	2022-01-10	7.5	CVE-2022-22823
libexpat_project -- libexpat	addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	2022-01-10	7.5	CVE-2022-22822
microsoft -- 365_apps	Microsoft Excel Remote Code Execution Vulnerability.	2022-01-11	9.3	CVE-2022-21841
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21855, CVE-2022-21969.	2022-01-11	8.3	CVE-2022-21846
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21846, CVE-2022-21969.	2022-01-11	7.7	CVE-2022-21855
microsoft -- sharepoint_foundation	Microsoft SharePoint Server Remote Code Execution Vulnerability.	2022-01-11	9	CVE-2022-21837
microsoft -- windows_10	Active Directory Domain Services Elevation of Privilege Vulnerability.	2022-01-11	9	CVE-2022-21857
microsoft -- windows_10	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21850.	2022-01-11	9.3	CVE-2022-21851
microsoft -- windows_10	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21851.	2022-01-11	9.3	CVE-2022-21850
microsoft -- windows_10	Windows IKE Extension Remote Code Execution Vulnerability.	2022-01-11	9.3	CVE-2022-21849
microsoft -- windows_10	Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-21843, CVE-2022-21883, CVE-2022-21889, CVE-2022-21890.	2022-01-11	7.1	CVE-2022-21848
microsoft -- windows_10	Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability.	2022-01-11	7.2	CVE-2022-21834
microsoft -- windows_10	Microsoft Cryptographic Services Elevation of Privilege Vulnerability.	2022-01-11	7.2	CVE-2022-21835
microsoft -- windows_10	Windows Certificate Spoofing Vulnerability.	2022-01-11	7.2	CVE-2022-21836
microsoft -- windows_10	Windows Cleanup Manager Elevation of Privilege Vulnerability.	2022-01-11	7.2	CVE-2022-21838
microsoft -- windows_10	Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21896, CVE-2022-21902.	2022-01-11	7.2	CVE-2022-21852
microsoft -- windows_10	Windows Bind Filter Driver Elevation of Privilege Vulnerability.	2022-01-11	7.2	CVE-2022-21858
microsoft -- windows_10	Task Flow Data Engine Elevation of Privilege Vulnerability.	2022-01-11	7.2	CVE-2022-21861
microsoft -- windows_10	Virtual Machine IDE Drive Elevation of Privilege Vulnerability.	2022-01-11	7.2	CVE-2022-21833
online_thesis_archiving_system_project --	Sourcecodester Online Thesis Archiving System 1.0 is vulnerable to SQL Injection. An attacker can bypass admin authentication and gain access to admin panel using SQL Injection	2022-01-10	7.5	CVE-2021-45334

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
online_thesis_archiving_system				
solarwinds -- serv-u	Serv-U web login screen was allowing characters that were not sanitized by the authentication mechanism. SolarWinds has updated the authentication mechanism to remedy this issue and prevent unauthorized parameters to be used in the Serv-U login screen With the Log4j issue in the wild, input fields across the internet have been tested for vulnerability. Although Serv-U was not affected by the log4j issue, It was discovered that better input validation could be implemented.	2022-01-10	7.5	CVE-2021-35247
trendmicro -- apex_one	A origin validation error vulnerability in Trend Micro Apex One (on-prem and SaaS) could allow a local attacker drop and manipulate a specially crafted file to issue commands over a certain pipe and elevate to a higher level of privileges. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2022-01-10	7.2	CVE-2021-45441
trendmicro -- apex_one	A unnecessary privilege vulnerability in Trend Micro Apex One and Trend Micro Worry-Free Business Security 10.0 SP1 (on-prem versions only) could allow a local attacker to abuse an impersonation privilege and elevate to a higher level of privileges. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2022-01-10	7.2	CVE-2021-45440
trendmicro -- apex_one	A link following privilege escalation vulnerability in Trend Micro Apex One (on-prem and SaaS) and Trend Micro Worry-Free Business Security (10.0 SP1 and Services) could allow a local attacker to create a specially crafted file with arbitrary content which could grant local privilege escalation on the affected system. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2022-01-10	7.2	CVE-2021-45231

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accesspressthemes --	The Cookie Notification Plugin for WordPress plugin before 1.0.9 does not sanitise or escape the id GET parameter before using it in a SQL statement, when retrieving	2022-01-24	6.5	CVE-2021-24858

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wp_cookie_user_info	the setting to edit in the admin dashboard, leading to an authenticated SQL Injection			
acf-extended -- advanced_custom_fields\	The Advanced Custom Fields: Extended WordPress plugin before 0.8.8.7 does not validate the order and orderby parameters before using them in a SQL statement, leading to a SQL Injection issue	2022-01-24	6.5	CVE-2021-24865
adodb_project -- adodb	Authentication Bypass by Primary Weakness in GitHub repository adodb/adodb prior to 5.20.21.	2022-01-25	6.4	CVE-2021-3850
appcms -- appcms	AppCMS 2.0.101 has a XSS injection vulnerability in \templates\m\inc_head.php	2022-01-23	4.3	CVE-2021-45380
asgaros -- asgaros_forum	The Asgaros Forum WordPress plugin before 1.15.15 does not validate or escape the forum_id parameter before using it in a SQL statement when editing a forum, leading to an SQL injection issue	2022-01-24	6.5	CVE-2021-25045
bingrep_project -- bingrep	Bingrep v0.8.5 was discovered to contain a memory allocation failure which can cause a Denial of Service (DoS).	2022-01-21	5	CVE-2021-39480
camunda -- min-dash	The package min-dash before 3.8.1 are vulnerable to Prototype Pollution via the set method due to missing enforcement of key types.	2022-01-21	5	CVE-2021-23460
codeigniter -- codeigniter	CodeIgniter4 is the 4.x branch of CodeIgniter, a PHP full-stack web framework. A cross-site scripting (XSS) vulnerability was found in `API\ResponseTrait` in Codeigniter4 prior to version 4.1.8. Attackers can do XSS attacks if a potential victim is using `API\ResponseTrait`. Version 4.1.8 contains a patch for this vulnerability. There are two potential workarounds available. Users may avoid using `API\ResponseTrait` or `ResourceController` Users may also disable Auto Route and use defined routes only.	2022-01-24	4.3	CVE-2022-21715
codesnippets -- code_snippets	The Code Snippets WordPress plugin before 2.14.3 does not escape the snippets-safe-mode parameter before outputting it back in attributes, leading to a Reflected Cross-Site Scripting issue	2022-01-24	4.3	CVE-2021-25008
coins-global -- construction_cloud	An issue was discovered in COINS Construction Cloud 11.12. Due to improper validation of user-controlled HTTP headers, attackers can cause it to send password-reset e-mails pointing to arbitrary websites.	2022-01-24	4.3	CVE-2021-45226
coins-global -- construction_cloud	An issue was discovered in COINS Construction Cloud 11.12. Due to improper input neutralization, it is vulnerable to reflected cross-site scripting (XSS) via malicious links (affecting the search window and activity view window).	2022-01-24	4.3	CVE-2021-45225
coins-global -- construction_cloud	An issue was discovered in COINS Construction Cloud 11.12. In several locations throughout the application, JavaScript code is passed as a URL parameter. Attackers can trivially alter this code to cause malicious behaviour. The application is therefore vulnerable to reflected XSS via malicious URLs.	2022-01-24	4.3	CVE-2021-45224
coins-global -- construction_cloud	An issue was discovered in COINS Construction Cloud 11.12. Due to logical flaws in the human ressources interface, it is vulnerable to privilege escalation by HR personnel.	2022-01-24	6.5	CVE-2021-45222
coins-global -- construction_cloud	An issue was discovered in COINS Construction Cloud 11.12. Due to insufficient input neutralization, it is vulnerable to denial of service attacks via forced server crashes.	2022-01-24	4	CVE-2021-45223
conda_loguru_project -- conda_loguru	Improper Privilege Management in Conda loguru prior to 0.5.3.	2022-01-25	4	CVE-2022-0338

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
contribsys -- sidekiq	In api.rb in Sidekiq before 6.4.0, there is no limit on the number of days when requesting stats for the graph. This overloads the system, affecting the Web UI, and makes it unavailable to users.	2022-01-21	5	CVE-2022-23837
convert-svg-core_project -- convert-svg-core	This affects all versions of package convert-svg-core; all versions of package convert-svg-to-png; all versions of package convert-svg-to-jpeg. Using a specially crafted SVG file, an attacker could read arbitrary files from the file system and then show the file content as a converted PNG file.	2022-01-21	5	CVE-2021-23631
crmperks -- contact_form_entries	The Contact Form Entries WordPress plugin before 1.2.4 does not sanitise and escape various parameters, such as form_id, status, end_date, order, orderby and search before outputting them back in the admin page	2022-01-24	4.3	CVE-2021-25079
crmperks -- contact_form_entries	The Contact Form Entries WordPress plugin before 1.1.7 does not validate, sanitise and escape the IP address retrieved via headers such as CLIENT-IP and X-FORWARDED-FOR, allowing unauthenticated attackers to perform Cross-Site Scripting attacks against logged in admins viewing the created entry	2022-01-24	4.3	CVE-2021-25080
dell -- emc_appsync	Dell EMC AppSync versions 3.9 to 4.3 contain a clickjacking vulnerability in AppSync. A remote unauthenticated attacker could potentially exploit this vulnerability to trick the victim into executing state changing operations.	2022-01-21	5.8	CVE-2022-22552
dell -- emc_appsync	DELL EMC AppSync versions 3.9 to 4.3 use GET request method with sensitive query strings. An Adjacent, unauthenticated attacker could potentially exploit this vulnerability, and hijack the victim session.	2022-01-21	5.8	CVE-2022-22551
dell -- emc_data_protection_central	Dell EMC Data Protection Central version 19.5 contains an Improper Input Validation Vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service.	2022-01-24	5	CVE-2021-43588
dell -- emc_data_protection_central	Dell EMC Data Protection Central versions 19.5 and prior contain a Server Side Request Forgery vulnerability in the DPC DNS client processing. A remote malicious user could potentially exploit this vulnerability, allowing port scanning of external hosts.	2022-01-24	4	CVE-2021-36349
dell -- solutions_enabler	The Dell EMC Virtual Appliances before 9.2.2.2 contain undocumented user accounts. A local malicious user may potentially exploit this vulnerability to get privileged access to the virtual appliance.	2022-01-21	4.6	CVE-2021-36339
dell -- solutions_enabler	Unisphere for PowerMax versions prior to 9.2.2.2 contains a privilege escalation vulnerability. An adjacent malicious user could potentially exploit this vulnerability to escalate their privileges and access functionalities they do not have access to.	2022-01-21	5.2	CVE-2021-36338
elfspirit_project -- elfspirit	elfspirit is an ELF static analysis and injection framework that parses, manipulates, and camouflages ELF files. When analyzing the ELF file format in versions prior to 1.1, there is an out-of-bounds read bug, which can lead to application crashes or information leakage. By constructing a special format ELF file, the information of any address can be leaked. elfspirit version 1.1 contains a patch for this issue.	2022-01-24	5.8	CVE-2022-21711
epub2txt_project -- epub2txt	xhtml_translate_entity in xhtml.c in epub2txt (aka epub2txt2) through 2.02 allows a stack-based buffer overflow via a crafted EPUB document.	2022-01-23	6.8	CVE-2022-23850
forestblog_project -- forestblog	A problem was found in ForestBlog, as of 2021-12-29, there is a XSS vulnerability that can be injected through the nickname input box.	2022-01-25	4.3	CVE-2021-46034
fresenius-kabi -- agilia_connect_firmware	Vigilant Software Suite (Mastermed Dashboard) version 2.0.1.3 contains service credentials likely to be common across all instances. An attacker in possession of the password may gain privileges on all installations of this software.	2022-01-21	6.5	CVE-2021-44464
fresenius-kabi -- agilia_connect_firmware	The SSL/TLS configuration of Fresenius Kabi Agilia Link + version 3.0 has serious deficiencies that may allow an attacker to compromise SSL/TLS sessions in different ways. An attacker may be able to eavesdrop on transferred data, manipulate data	2022-01-21	6.4	CVE-2021-31562

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allegedly secured by SSL/TLS, and impersonate an entity to gain access to sensitive information.			
fresenius-kabi -- agilia_connect_firmware	Fresenius Kabi Vigilant Software Suite (Mastermed Dashboard) version 2.0.1.3 has the option for automated indexing (directory listing) activated. When accessing a directory, a web server delivers its entire content in HTML form. If an index file does not exist and directory listing is enabled, all content of the directory will be displayed, allowing an attacker to identify and access files on the server.	2022-01-21	5	CVE-2021-23195
fresenius-kabi -- agilia_connect_firmware	Fresenius Kabi Vigilant Software Suite (Mastermed Dashboard) version 2.0.1.3 is vulnerable to reflected cross-site scripting attacks. An attacker could inject JavaScript in a GET parameter of HTTP requests and perform unauthorized actions such as stealing internal information and performing actions in context of an authenticated user.	2022-01-21	4.3	CVE-2021-33848
fresenius-kabi -- agilia_connect_firmware	Fresenius Kabi Agilia SP MC WiFi vD25 and prior has a default configuration page accessible without authentication. An attacker may use this functionality to change the exposed configuration values such as network settings.	2022-01-21	5	CVE-2021-33843
fresenius-kabi -- agilia_partner_maintenance_software	Fresenius Kabi Agilia Link + version 3.0 does not enforce transport layer encryption. Therefore, transmitted data may be sent in cleartext. Transport layer encryption is offered on Port TCP/443, but the affected service does not perform an automated redirect from the unencrypted service on Port TCP/80 to the encrypted service.	2022-01-21	5	CVE-2021-41835
fresenius-kabi -- agilia_partner_maintenance_software	Fresenius Kabi Vigilant Software Suite (Mastermed Dashboard) version 2.0.1.3 issues authentication tokens to authenticated users that are signed with a symmetric encryption key. An attacker in possession of the key can issue valid JWTs and impersonate arbitrary users.	2022-01-21	6.5	CVE-2021-33846
golang -- go	In archive/zip in Go before 1.16.8 and 1.17.x before 1.17.1, a crafted archive header (falsely designating that many files are present) can cause a NewReader or OpenReader panic. NOTE: this issue exists because of an incomplete fix for CVE-2021-33196.	2022-01-24	5	CVE-2021-39293
gpac -- gpac	A NULL pointer dereference vulnerability exists in GPAC v1.1.0 via the function gf_dump_vrml_sffield () at scene_manager/scene_dump.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-21	4.3	CVE-2021-46240
gpac -- gpac	A NULL pointer dereference vulnerability exists in GPAC v1.1.0 via the function gf_node_unregister () at scenegraph/base_scenegraph.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-21	4.3	CVE-2021-46234
gpac -- gpac	A NULL pointer dereference vulnerability exists in GPAC v1.1.0 via the function gf_sg_vrml_field_pointer_del () at scenegraph/vrml_tools.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-21	4.3	CVE-2021-46236
gpac -- gpac	An untrusted pointer dereference vulnerability exists in GPAC v1.1.0 via the function gf_node_unregister () at scenegraph/base_scenegraph.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-21	4.3	CVE-2021-46237
gpac -- gpac	GPAC v1.1.0 was discovered to contain a stack overflow via the function gf_node_get_name () at scenegraph/base_scenegraph.c. This vulnerability can lead to a program crash, causing a Denial of Service (DoS).	2022-01-21	4.3	CVE-2021-46238
gpac -- gpac	The binary MP4Box in GPAC v1.1.0 was discovered to contain an invalid free vulnerability via the function gf_free () at utils/alloc.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-21	4.3	CVE-2021-46239
gpac -- gpac	The binary MP4Box in GPAC v1.0.1 was discovered to contain a segmentation fault via the function __memmove_avx_unaligned_erms (). This vulnerability can lead to a Denial of Service (DoS).	2022-01-21	4.3	CVE-2021-46313

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac -- gpac	A NULL pointer dereference vulnerability exists in GPAC v1.1.0 via the function gf_sg_destroy_routes () at scenegraph/vrml_route.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-21	4.3	CVE-2021-46311
hdfgroup -- hdf5	A Divide By Zero vulnerability exists in HDF5 v1.13.1-1 vis the function H5T__complete_copy () at /hdf5/src/H5T.c. This vulnerability causes an aritmetic exception, leading to a Denial of Service (DoS).	2022-01-21	4.3	CVE-2021-46244
hdfgroup -- hdf5	An untrusted pointer dereference vulnerability exists in HDF5 v1.13.1-1 via the function H5O__dtype_decode_helper () at hdf5/src/H5Odtype.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-21	4.3	CVE-2021-46243
hdfgroup -- hdf5	HDF5 v1.13.1-1 was discovered to contain a heap-use-after free via the component H5AC_unpin_entry.	2022-01-21	6.8	CVE-2021-46242
hospital\'s_patient_records_management_system_project -- hospital\'s_patient_records_management_system	Sourcecodester Hospital's Patient Records Management System 1.0 is vulnerable to Insecure Permissions via the id parameter in manage_user endpoint. Simply change the value and data of other users can be displayed.	2022-01-24	5	CVE-2022-22296
ibm -- cognos_controller	IBM Cognos Controller 10.4.0, 10.4.1, and 10.4.2 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 190839.	2022-01-21	6.4	CVE-2020-4876 XF
ibm -- cognos_controller	IBM Cognos Controller 10.4.0, 10.4.1, and 10.4.2 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 190838.	2022-01-21	6.4	CVE-2020-4875 XF
ibm -- websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 22.0.0.1 could allow a remote authenticated attacker to conduct an LDAP injection. By using a specially crafted request, an attacker could exploit this vulnerability and could result in in granting permission to unauthorized resources. IBM X-Force ID: 213875.	2022-01-25	6.5	CVE-2021-39031 XF
iconics -- genesis64	Buffer Over-read vulnerability in Mitsubishi Electric MC Works64 versions 4.00A (10.95.201.23) to 4.04E (10.95.210.01), ICONICS GENESIS64 versions 10.97 and prior and ICONICS Hyper Historian versions 10.97 and prior allows an attacker to cause a DoS condition in the database server by getting a legitimate user to import a configuration file containing specially crafted stored procedures into GENESIS64 or MC Works64 and execute commands against the database from GENESIS64 or MC Works64.	2022-01-21	4.3	CVE-2022-23130
iconics -- mobilehmi	Cross-site Scripting vulnerability in Mitsubishi Electric MC Works64 versions 4.04E (10.95.210.01) and prior and ICONICS MobileHMI versions 10.96.2 and prior allows a remote unauthenticated attacker to gain authentication information of an MC Works64 or MobileHMI and perform any operation using the acquired authentication information, by injecting a malicious script in the URL of a monitoring screen delivered from the MC Works64 server or MobileHMI server to an application for mobile devices and leading a legitimate user to access this URL.	2022-01-21	4.3	CVE-2022-23127
iresturant_project -- iresturant	MartDevelopers iResturant 1.0 is vulnerable to SQL Injection. SQL Injection occurs because this view parameter value is added to the SQL query without additional verification when viewing reservation.	2022-01-25	6.5	CVE-2021-45803
isomorphic-git -- cors-proxy	The package @isomorphic-git/cors-proxy before 2.7.1 are vulnerable to Server-side Request Forgery (SSRF) due to missing sanitization and validation of the redirection action in middleware.js.	2022-01-21	5	CVE-2021-23664

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jerryscript -- jerryscript	Jerryscript 3.0.0 was discovered to contain a stack overflow via ecma_lcache_lookup in /jerry-core/ecma/base/ecma-lcache.c.	2022-01-21	6.8	CVE-2022-22894
jerryscript -- jerryscript	Jerryscript 3.0.0 was discovered to contain a SEGV vulnerability via ecma_ref_object_inline in /jerry-core/ecma/base/ecma-gc.c.	2022-01-21	4.3	CVE-2022-22891
jerryscript -- jerryscript	There is an Assertion 'ecma_is_value_undefined (value) || ecma_is_value_null (value) || ecma_is_value_boolean (value) || ecma_is_value_number (value) || ecma_is_value_string (value) || ecma_is_value_bigint (value) || ecma_is_value_symbol (value) || ecma_is_value_object (value)' failed at jerry-core/ecma/base/ecma-helpers-value.c in Jerryscripts 3.0.0.	2022-01-21	4.3	CVE-2022-22892
jerryscript -- jerryscript	There is an Assertion ''ecma_object_is_typedarray (obj_p)'' failed at /jerry-core/ecma/operations/ecma-typedarray-object.c in Jerryscript 3.0.0.	2022-01-25	4.3	CVE-2021-44992
jerryscript -- jerryscript	Jerryscript 3.0.0 was discovered to contain a stack overflow via vm_loop.lto_priv.304 in /jerry-core/vm/vm.c.	2022-01-21	6.8	CVE-2022-22893
jerryscript -- jerryscript	Jerryscript 3.0.0 was discovered to contain a heap-buffer-overflow via ecma_utf8_string_to_number_by_radix in /jerry-core/ecma/base/ecma-helpers-conversion.c.	2022-01-21	6.8	CVE-2022-22895
jerryscript -- jerryscript	Jerryscript v3.0.0 and below was discovered to contain a stack overflow via ecma_find_named_property in ecma-helpers.c.	2022-01-25	6.8	CVE-2021-44988
jerryscript -- jerryscript	There is an Assertion ''JERRY_CONTEXT (jmem_heap_allocated_size) == 0'' failed at /jerry-core/jmem/jmem-heap.c in Jerryscript 3.0.0.	2022-01-25	4.3	CVE-2021-44994
jerryscript -- jerryscript	There is an Assertion ''ecma_is_value_boolean (base_value)'' failed at /jerry-core/ecma/operations/ecma-get-put-value.c in Jerryscript 3.0.0.	2022-01-25	4.3	CVE-2021-44993
jsish -- jsish	Jsish v3.5.0 was discovered to contain a heap buffer overflow via NumberConstructor at src/jsiNumber.c.	2022-01-25	6.8	CVE-2021-46482
jsish -- jsish	Jsish v3.5.0 was discovered to contain a heap buffer overflow via jsiValueObjDelete in src/jsiEval.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-25	4.3	CVE-2021-46480
jsish -- jsish	Jsish v3.5.0 was discovered to contain a memory leak via linenoise at src/linenoise.c.	2022-01-25	4.3	CVE-2021-46481
jsish -- jsish	Jsish v3.5.0 was discovered to contain a heap buffer overflow via RegExp_constructor in src/jsiRegexp.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-25	4.3	CVE-2021-46477
jsish -- jsish	Jsish v3.5.0 was discovered to contain a heap buffer overflow via BooleanConstructor at src/jsiBool.c.	2022-01-25	6.8	CVE-2021-46483
jsish -- jsish	Jsish v3.5.0 was discovered to contain a heap buffer overflow via jsiEvalCodeSub in src/jsiEval.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-25	4.3	CVE-2021-46474
jsish -- jsish	Jsish v3.5.0 was discovered to contain a heap buffer overflow via jsiClearStack in src/jsiEval.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-25	4.3	CVE-2021-46478
jsish -- jsish	Jsish v3.5.0 was discovered to contain a heap buffer overflow via jsi_ArraySliceCmd in src/jsiArray.c. This vulnerability can lead to a Denial of Service (DoS).	2022-01-25	4.3	CVE-2021-46475
kea-hotel-erp_project -- kea-hotel-erp	In MartDevelopers KEA-Hotel-ERP open source as of 12-31-2021, a remote code execution vulnerability can be exploited by uploading PHP files using the file upload vulnerability in this service.	2022-01-25	6.5	CVE-2021-46113
librecad -- librecad	In LibreCAD 2.2.0, a NULL pointer dereference in the HATCH handling of libdxfrw allows an attacker to crash the application using a crafted DXF document.	2022-01-25	4.3	CVE-2021-45343

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
librecad -- librecad	A buffer overflow vulnerability in CDataList of the jwwlib component of LibreCAD 2.2.0-rc3 and older allows an attacker to achieve Remote Code Execution using a crafted JWW document.	2022-01-25	6.8	CVE-2021-45342
libsixel_project -- libsixel	In Libsixel prior to and including v1.10.3, a NULL pointer dereference in the stb_image.h component of libsixel allows attackers to cause a denial of service (DOS) via a crafted PICT file.	2022-01-25	4.3	CVE-2021-45340
linux -- linux_kernel	A race condition was found in the Linux kernel's ebpf verifier between bpf_map_update_elem and bpf_map_freeze due to a missing lock in kernel/bpf/syscall.c. In this flaw, a local user with a special privilege (cap_sys_admin or cap_bpf) can modify the frozen mapped address space. This flaw affects kernel versions prior to 5.16 rc2.	2022-01-21	4.7	CVE-2021-4001
linux -- linux_kernel	A vulnerability was found in the Linux kernel's KVM subsystem in arch/x86/kvm/lapic.c kvm_free_lapic when a failure allocation was detected. In this flaw the KVM subsystem may crash the kernel due to mishandling of memory errors that happens during VCPU construction, which allows an attacker with special user privilege to cause a denial of service. This flaw affects kernel versions prior to 5.15 rc7.	2022-01-21	4.9	CVE-2021-4032
mcafee -- data_loss_prevention	SQL injection vulnerability in Data Loss Protection (DLP) ePO extension 11.8.x prior to 11.8.100, 11.7.x prior to 11.7.101, and 11.6.401 allows a remote authenticated attacker to inject unfiltered SQL into the DLP part of the ePO database. This could lead to remote code execution on the ePO server with privilege escalation.	2022-01-24	6.5	CVE-2021-4088
mediawiki -- shortdescription	ShortDescription is a MediaWiki extension that provides local short description support. A cross-site scripting (XSS) vulnerability exists in versions prior to 2.3.4. On a wiki that has the ShortDescription enabled, XSS can be triggered on any page or the page with the action=info parameter, which displays the shortdesc property. This is achieved using the wikitext `{{SHORTDESC:&lt;img src=x onerror=alert()&gt;}}`. This issue has a patch in version 2.3.4.	2022-01-24	4.3	CVE-2022-21710
mruby -- mruby	NULL Pointer Dereference in Homebrew mruby prior to 3.2.	2022-01-21	4.3	CVE-2022-0326
mustache_project -- mustache	Improper Neutralization of Special Elements Used in a Template Engine in Packagist mustache/mustache prior to 2.14.1.	2022-01-21	6.5	CVE-2022-0323
mycred -- mycred	The myCred WordPress plugin before 2.4 does not sanitise and escape the search query before outputting it back in the history dashboard page, leading to a Reflected Cross-Site Scripting issue	2022-01-24	4.3	CVE-2021-25015
navidrome -- navidrome	model/criteria/criteria.go in Navidrome before 0.47.5 is vulnerable to SQL injection attacks when processing crafted Smart Playlists. An authenticated user could abuse this to extract arbitrary data from the database, including the user table (which contains sensitive information such as the users' encrypted passwords).	2022-01-24	4	CVE-2022-23857
nlnetlabs -- ldns	When a zone file in ldns 1.7.1 is parsed, the function ldns_nsec3_salt_data is too trusted for the length value obtained from the zone file. When the memcpy is copied, the 0xfe - ldns_rdf_size(salt_rdf) byte data can be copied, causing heap overflow information leakage.	2022-01-21	5	CVE-2020-19861
nlnetlabs -- ldns	When ldns version 1.7.1 verifies a zone file, the ldns_rr_new_frm_str_internal function has a heap out of bounds read vulnerability. An attacker can leak information on the heap by constructing a zone file payload.	2022-01-21	4.3	CVE-2020-19860
online_covid_vaccination_scheduler_system_project -- online_covid_vaccination_scheduler_system	Cross site scripting (XSS) vulnerability in Sourcecodester Online Covid Vaccination Scheduler System v1 by oretnom23, allows attackers to execute arbitrary code via the lid parameter to /scheduler/addSchedule.php.	2022-01-24	4.3	CVE-2021-41930

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oxilab -- image_hover_effects_ultimate	The Image Hover Effects Ultimate (Image Gallery, Effects, Lightbox, Comparison or Magnifier) WordPress plugin before 9.7.1 does not escape the effects parameter before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting	2022-01-24	4.3	CVE-2021-25031
php_crud_without_refresh\/reload_using_ajax_and_datatables_tutorial_project -- php_crud_without_refresh\/reload_using_ajax_and_datatables_tutorial	Cross site scripting (XSS) vulnerability in sourcecodester PHP CRUD without Refresh/Reload using Ajax and DataTables Tutorial v1 by oretnom23, allows remote attackers to execute arbitrary code via the first_name, last_name, and email parameters to /ajax_crud.	2022-01-24	6.8	CVE-2021-40909
phpmyadmin -- phpmyadmin	An issue was discovered in phpMyAdmin 5.1 before 5.1.2. An attacker can inject malicious code into aspects of the setup script, which can allow XSS or HTML injection.	2022-01-22	4.3	CVE-2022-23808
phpmyadmin -- phpmyadmin	An issue was discovered in phpMyAdmin 4.9 before 4.9.8 and 5.1 before 5.1.2. A valid user who is already authenticated to phpMyAdmin can manipulate their account to bypass two-factor authentication for future login instances.	2022-01-22	4	CVE-2022-23807
plutinosoft -- platinum	Platinum Upnp SDK through 1.2.0 has a directory traversal vulnerability. The attack could remote attack victim by sending http://ip:port/../privacy.avi URL to compromise a victim's privacy.	2022-01-21	5	CVE-2020-19858
revmakx -- backup_and_staging_by_wp_time_capsule	The Backup and Staging by WP Time Capsule WordPress plugin before 1.22.7 does not sanitise and escape the error parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting	2022-01-24	4.3	CVE-2021-25035
roundupwp -- registrations_for_the_events_calendar	The Registrations for the Events Calendar WordPress plugin before 2.7.10 does not escape the qtype parameter before outputting it back in an attribute in the settings page, leading to a Reflected Cross-Site Scripting	2022-01-24	4.3	CVE-2021-25083
saviynt -- enterprise_identity_cloud	An issue was discovered in Saviynt Enterprise Identity Cloud (EIC) 5.5 SP2.x. An attacker can enumerate users by changing the id parameter, such as for the ECM/maintenance/forgotpasswordstep1 URI.	2022-01-24	5	CVE-2022-23856
sendinblue -- newsletter\,_smtp\,_email_marketing_and_subscribe	The Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue WordPress plugin before 3.1.25 does not escape the sib-statistics-date parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting issue	2022-01-24	4.3	CVE-2021-24923
simple_college_website_project -- simple_college_website	Simple College Website 1.0 is vulnerable to unauthenticated file upload & remote code execution via UNION-based SQL injection in the username parameter on /admin/login.php.	2022-01-21	6.8	CVE-2021-44593
slic3r -- slic3r	A flaw in the AMF parser of Slic3r libslic3r 1.3.0 allows an attacker to cause an application crash using a crafted AMF document, where a metadata tag lacks a "type" attribute.	2022-01-25	4.3	CVE-2021-45846
slic3r -- slic3r	Several missing input validations in the 3MF parser component of Slic3r libslic3r 1.3.0 can each allow an attacker to cause an application crash using a crafted 3MF input file.	2022-01-25	4.3	CVE-2021-45847
themeum -- qubely	The Qubely WordPress plugin before 1.7.8 does not have authorisation and CSRF check on the qubely_delete_saved_block AJAX action, and does not ensure that	2022-01-24	4	CVE-2021-25013

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the block to be deleted belong to the plugin, as a result, any authenticated users, such as subscriber can delete arbitrary posts			
themeum -- tutor_lms	The Tutor LMS WordPress plugin before 1.9.12 does not escape the search parameter before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting	2022-01-24	4.3	CVE-2021-25017
tipsandtricks-hq -- simple_download_monitor	The Simple Download Monitor WordPress plugin before 3.9.9 does not enforce nonce checks, which could allow attackers to perform CSRF attacks to 1) make admins export logs to exploit a separate log disclosure vulnerability (fixed in 3.9.6), 2) delete logs (fixed in 3.9.9), 3) remove thumbnail image from downloads	2022-01-24	6.8	CVE-2021-24696
tri -- event_tickets	The Event Tickets WordPress plugin before 5.2.2 does not validate the tribe_tickets_redirect_to parameter before redirecting the user to the given value, leading to an arbitrary redirect issue	2022-01-24	5.8	CVE-2021-25028
try_my_recipe_project -- try_my_recipe	Cross Site Scripting (XSS) in Sourcecodester Try My Recipe (Recipe Sharing Website - CMS) by oretnom23, allows attackers to gain the PHPSESID or other unspecified impacts via the fullname parameter to the login_registration page.	2022-01-24	4.3	CVE-2021-42168
villatheme -- orders_tracking_for_woocommerce	The Orders Tracking for WooCommerce WordPress plugin before 1.1.10 does not sanitise and escape the file_url before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting	2022-01-24	4.3	CVE-2021-25062
vim -- vim	Out-of-bounds Read in vim/vim prior to 8.2.	2022-01-21	4.3	CVE-2022-0319
wasmcloud -- host_runtime	wasmCloud Host Runtime is a server process that securely hosts and provides dispatch for web assembly (WASM) actors and capability providers. In versions prior to 0.52.2 actors can bypass capability authorization. Actors are normally required to declare their capabilities for inbound invocations, but with this vulnerability actor capability claims are not verified upon receiving invocations. This compromises the security model for actors as they can receive unauthorized invocations from linked capability providers. The problem has been patched in versions `0.52.2` and greater. There is no workaround and users are advised to upgrade to an unaffected version as soon as possible.	2022-01-21	5.5	CVE-2022-21707
webmaster-source -- wp125	The WP125 WordPress plugin before 1.5.5 does not have CSRF checks in various action, for example when deleting an ad, allowing attackers to make a logged in admin delete them via a CSRF attack	2022-01-24	6.8	CVE-2021-25073
webp_converter_for_media_project -- webp_converter_for_media	The WebP Converter for Media WordPress plugin before 4.0.3 contains a file (passthru.php) which does not validate the src parameter before redirecting the user to it, leading to an Open Redirect issue	2022-01-24	5.8	CVE-2021-25074
wp-experts -- protect_wp_admin	The Protect WP Admin WordPress plugin before 3.6.2 does not check for authorisation in the lib/pwa-deactivate.php file, which could allow unauthenticated users to disable the plugin (and therefore the protection offered) via a crafted request	2022-01-24	5	CVE-2021-24906
wp_extra_file_types_project -- wp_extra_file_types	The WP Extra File Types WordPress plugin before 0.5.1 does not have CSRF check when saving its settings, nor sanitise and escape some of them, which could allow attackers to make a logged in admin change them and perform Cross-Site Scripting attacks	2022-01-24	6	CVE-2021-24936
wp_post_page_clone_project -- wp_post_page_clone	The WP Post Page Clone WordPress plugin before 1.2 allows users with a role as low as Contributor to clone and view other users' draft and password-protected posts which they cannot view normally.	2022-01-24	4	CVE-2021-24733

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpaffiliatemanager -- affiliates_manager	The Affiliates Manager WordPress plugin before 2.9.0 does not validate, sanitise and escape the IP address of requests logged by the click tracking feature, allowing unauthenticated attackers to perform Cross-Site Scripting attacks against admin viewing the tracked requests.	2022-01-24	4.3	CVE-2021-25078
wpplugin -- accept_donations_with_paypal	The Accept Donations with PayPal WordPress plugin before 1.3.4 does not have CSRF check in place and does not ensure that the post to be deleted belongs to the plugin, allowing attackers to make a logged in admin delete arbitrary posts from the blog	2022-01-24	4.3	CVE-2021-24989
yetiforce -- yetiforce_customer_relationship_management	Cross-Site Request Forgery (CSRF) in Packagist yetiforce/yetiforce-crm prior to 6.3.0.	2022-01-24	6	CVE-2022-0269
yikesinc -- easy_forms_for_mailchimp	The Easy Forms for Mailchimp WordPress plugin before 6.8.6 does not sanitise and escape the field_name and field_type parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues	2022-01-24	4.3	CVE-2021-24985
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Access of Memory Location After End of Buffer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-45067
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-45063
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Access of Memory Location After End of Buffer vulnerability that could lead to application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-44712
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in application denial of service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-44713
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a Violation of Secure Design Principles that could lead to a Security feature bypass. Acrobat Reader DC displays a warning message when a user clicks on a PDF file, which could be used by an attacker to mislead the user. In affected versions, this warning message does not include custom protocols when used by the sender. User interaction is required to abuse this vulnerability as they would need to click 'allow' on the warning message of a malicious file.	2022-01-14	4.3	CVE-2021-44714
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-44715

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	6.8	CVE-2021-45064
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	6.8	CVE-2021-45068
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-44740
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-44741
adobe -- acrobat_dc	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-44742
adobe -- bridge	Adobe Bridge version 11.1.2 (and earlier) and version 12.0 (and earlier) are affected by an use-after-free vulnerability in the processing of Format event actions that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-45051
adobe -- bridge	Adobe Bridge version 11.1.2 (and earlier) and version 12.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious TIF file.	2022-01-14	4.3	CVE-2021-45052
adobe -- illustrator	Adobe Illustrator versions 25.4.2 (and earlier) and 26.0.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-43752
adobe -- illustrator	Adobe Illustrator versions 25.4.2 (and earlier) and 26.0.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-14	4.3	CVE-2021-44700
alcoda -- netbiblio	Cross-site Scripting (XSS) vulnerability in the search functionality of AlCoda NetBiblio WebOPAC allows an unauthenticated user to craft a reflected Cross-Site Scripting attack. This issue affects: AlCoda NetBiblio WebOPAC versions prior to	2022-01-14	4.3	CVE-2021-42551

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	4.0.0.320; versions later than 4.0.0.328. This issue does not affect: AlCoda NetBiblio WebOPAC version 4.0.0.335 and later versions.			
arista -- eos	An issue has recently been discovered in Arista EOS where the incorrect use of EOS's AAA API's by the OpenConfig and TerminAttr agents could result in unrestricted access to the device for local users with nopassword configuration.	2022-01-14	6.9	CVE-2021-28500
arista -- terminattr	An issue has recently been discovered in Arista EOS where the incorrect use of EOS's AAA API's by the OpenConfig and TerminAttr agents could result in unrestricted access to the device for local users with nopassword configuration.	2022-01-14	6.9	CVE-2021-28501
calibre-web_project -- calibre-web	calibre-web is vulnerable to Cross-Site Request Forgery (CSRF)	2022-01-17	6.8	CVE-2021-4164
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20643 CISCO
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20647 CISCO
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20646 CISCO
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20645 CISCO
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20644 CISCO

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20635 CISCO
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20642 CISCO
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20641 CISCO
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20640 CISCO
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20639 CISCO
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20638 CISCO
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute	2022-01-14	4.3	CVE-2022-20637 CISCO

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary script code in the context of the interface or access sensitive, browser-based information.			
cisco -- security_manager	Multiple vulnerabilities in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 interface or access sensitive, browser-based information.	2022-01-14	4.3	CVE-2022-20636 CISCO
clamav -- clamav	A vulnerability in the OOXML parsing module in Clam AntiVirus (ClamAV) Software version 0.104.1 and LTS version 0.103.4 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper checks that may result in an invalid pointer read. An attacker could exploit this vulnerability by sending a crafted OOXML file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process to crash, resulting in a denial of service condition.	2022-01-14	5	CVE-2022-20698 CISCO
colors.js_project -- colors.js	The package colors after 1.4.0 are vulnerable to Denial of Service (DoS) that was introduced through an infinite loop in the americanFlag module. Unfortunately this appears to have been a purposeful attempt by a maintainer of colors to make the package unusable, other maintainers' controls over this package appear to have been revoked in an attempt to prevent them from fixing the issue. Vulnerable Code js for (let i = 666; i < Infinity; i++;) { Alternative Remediation Suggested * Pin dependancy to 1.4.0	2022-01-14	5	CVE-2021-23567
discourse -- discourse	Discourse is an open source discussion platform. Discourse groups can be configured with varying visibility levels for the group as well as the group members. By default, a newly created group has its visibility set to public and the group's members visibility set to public as well. However, a group's visibility and the group's members visibility can be configured such that it is restricted to logged on users, members of the group or staff users. A vulnerability has been discovered in versions prior to 2.7.13 and 2.8.0.beta11 where the group advanced search option does not respect the group's visibility and members visibility level. As such, a group with restricted visibility or members visibility can be revealed through search with the right search option. This issue is patched in `stable` version 2.7.13, `beta` version 2.8.0.beta11, and `tests-passed` version 2.8.0.beta11 versions of Discourse. There are no workarounds aside from upgrading.	2022-01-14	5	CVE-2022-21677
eyoucms -- eyoucms	eyouCMS V1.5.5-UTF8-SP3_1 suffers from Arbitrary file deletion due to insufficient filtering of the parameter filename.	2022-01-14	5.5	CVE-2021-46255
futurepress -- epub.js	managers/views/iframe.js in FuturePress EPub.js before 0.3.89 allows XSS.	2022-01-17	4.3	CVE-2021-33040
gnu -- gcc	GCC v12.0 was discovered to contain an uncontrolled recursion via the component libiberty/rust-demangle.c. This vulnerability allows attackers to cause a Denial of Service (DoS) by consuming excessive CPU and memory resources.	2022-01-14	4.3	CVE-2021-46195
gnu -- recutils	An Use-After-Free vulnerability in rec_mset_elem_destroy() at rec-mset.c of GNU Recutils v1.8.90 can lead to a segmentation fault or application crash.	2022-01-14	4.3	CVE-2021-46022
gnu -- recutils	An untrusted pointer dereference in rec_db_destroy() at rec-db.c of GNU Recutils v1.8.90 can lead to a segmentation fault or application crash.	2022-01-14	4.3	CVE-2021-46019
gnu -- recutils	An Use-After-Free vulnerability in rec_record_destroy() at rec-record.c of GNU Recutils v1.8.90 can lead to a segmentation fault or application crash.	2022-01-14	4.3	CVE-2021-46021

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In phTmlNfc_Init and phTmlNfc_CleanUp of phTmlNfc.cc, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-197353344	2022-01-14	6.9	CVE-2021-39629
google -- android	In init of vendor_graphicbuffer_meta.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-188745089References: N/A	2022-01-14	6.9	CVE-2021-39679
google -- android	In LocationSettingsActivity of AndroidManifest.xml, there is a possible EoP due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-182812255	2022-01-14	6.8	CVE-2021-1036
google -- android	The broadcast that DevicePickerFragment sends when a new device is paired doesn't have any permission checks, so any app can register to listen for it. This lets apps keep track of what devices are paired without requesting BLUETOOTH permissions.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-162951906	2022-01-14	5	CVE-2021-1037
google -- android	In delete_protocol of main.c, there is a possible arbitrary code execution 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.Product: AndroidVersions: Android kernelAndroid ID: A-200251074References: N/A	2022-01-14	4.6	CVE-2021-39681
google -- android	In sortSimPhoneAccountsForEmergency of CreateConnectionProcessor.java, there is a possible prevention of access to emergency calling due to an unhandled exception. In rare instances, this could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-208267659	2022-01-14	4.7	CVE-2021-39659
gpac -- gpac	GPAC v1.1.0 was discovered to contain an invalid memory address dereference via the function gf_list_last(). This vulnerability allows attackers to cause a Denial of Service (DoS).	2022-01-14	4.3	CVE-2021-45760
gpac -- gpac	GPAC v1.1.0 was discovered to contain an invalid call in the function gf_node_changed(). This vulnerability can lead to a Denial of Service (DoS).	2022-01-14	4.3	CVE-2021-45763
gpac -- gpac	GPAC v1.1.0 was discovered to contain an invalid memory address dereference via the function shift_chunk_offsets.isra().	2022-01-14	4.3	CVE-2021-45764
gpac -- gpac	GPAC 1.1.0 was discovered to contain an invalid memory address dereference via the function lsr_read_id(). This vulnerability can lead to a Denial of Service (DoS).	2022-01-14	4.3	CVE-2021-45767
gpac -- gpac	GPAC v1.1.0 was discovered to contain an invalid memory address dereference via the function gf_sg_vrml_mf_reset(). This vulnerability allows attackers to cause a Denial of Service (DoS).	2022-01-14	4.3	CVE-2021-45762
jerryscript -- jerryscript	An issue was discovered in JerryScript commit a6ab5e9. There is an Use-After-Free in lexer_compare_identifier_to_string in js-lexer.c file.	2022-01-14	5	CVE-2021-46170
johnsoncontrols -- videoedge	Running a vulnerability scanner against VideoEdge NVRs can cause some functionality to stop.	2022-01-14	5	CVE-2021-36199 CERT
livehelperchat -- live_helper_chat	livehelperchat is vulnerable to Cross-Site Request Forgery (CSRF)	2022-01-14	4.3	CVE-2022-0231

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
livehelperchat -- live_helper_chat	livehelperchat is vulnerable to Cross-Site Request Forgery (CSRF)	2022-01-14	4.3	CVE-2022-0226
microfocus -- arcsight_enterprise_security_manager	Potential vulnerabilities have been identified in Micro Focus ArcSight Enterprise Security Manager, affecting versions 7.4.x and 7.5.x. The vulnerabilities could be remotely exploited resulting in Cross-Site Scripting (XSS).	2022-01-14	4.3	CVE-2021-38126
microfocus -- arcsight_enterprise_security_manager	Potential vulnerabilities have been identified in Micro Focus ArcSight Enterprise Security Manager, affecting versions 7.4.x and 7.5.x. The vulnerabilities could be remotely exploited resulting in Cross-Site Scripting (XSS).	2022-01-14	4.3	CVE-2021-38127
modex_project -- modex	Modex v2.11 was discovered to contain a NULL pointer dereference in set_create_id() at xtract.c.	2022-01-14	4.3	CVE-2021-46171
modex_project -- modex	Modex v2.11 was discovered to contain an Use-After-Free vulnerability via the component tcache.	2022-01-14	4.3	CVE-2021-46169
mruby -- mruby	An untrusted pointer dereference in mrb_vm_exec() of mruby v3.0.0 can lead to a segmentation fault or application crash.	2022-01-14	5	CVE-2021-46020
mz-automation -- lib60870	A NULL pointer dereference in CS104_IPAddress_setFromString at src/iec60870/cs104/cs104_slave.c of lib60870 commit 0d5e76e can lead to a segmentation fault or application crash.	2022-01-14	5	CVE-2021-45773
mz-automation -- libiec61850	A NULL pointer dereference in AcseConnection_parseMessage at src/mms/iso_acse/acse.c of libiec61850 v1.5.0 can lead to a segmentation fault or application crash.	2022-01-14	5	CVE-2021-45769
node-fetch_project -- node-fetch	node-fetch is vulnerable to Exposure of Sensitive Information to an Unauthorized Actor	2022-01-16	5.8	CVE-2022-0235
octobercms -- october	October CMS is a self-hosted content management system (CMS) platform based on the Laravel PHP Framework. Prior to versions 1.0.473 and 1.1.6, an attacker with access to the backend is able to execute PHP code by using the theme import feature. This will bypass the safe mode feature that prevents PHP execution in the CMS templates.The issue has been patched in Build 473 (v1.0.473) and v1.1.6. Those unable to upgrade may apply the patch to their installation manually as a workaround.	2022-01-14	6.5	CVE-2021-32650
omron -- cx-one	Omron CX-One Versions 4.60 and prior are vulnerable to a stack-based buffer overflow while processing specific project files, which may allow an attacker to execute arbitrary code.	2022-01-14	6.8	CVE-2022-21137
opendesign -- drawings_software_development_kit	Open Design Alliance Drawings SDK before 2022.12.1 mishandles the loading of JPG files. Unchecked input data from a crafted JPG file leads to memory corruption. An attacker can leverage this vulnerability to execute code in the context of the current process.	2022-01-15	6.8	CVE-2022-23095
oracle -- communications_billing_and_revenue_management	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Pipeline Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications Billing and Revenue Management accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2022-01-19	5	CVE-2022-21266
oracle -- communications_b	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily	2022-01-19	6.5	CVE-2022-21276

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
illing_and_revenue_management	exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in Oracle Communications Billing and Revenue Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).			
oracle -- communications_operations_monitor	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Operations Monitor, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Operations Monitor accessible data as well as unauthorized read access to a subset of Oracle Communications Operations Monitor 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).	2022-01-19	4.9	CVE-2022-21246
oracle -- configurator	Vulnerability in the Oracle Configurator product of Oracle E-Business Suite (component: UI Servlet). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Configurator accessible data as well as unauthorized access to critical data or complete access to all Oracle Configurator accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2022-01-19	5.5	CVE-2022-21255
oracle -- database_server	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Session, Execute Catalog Role privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2022-01-19	4	CVE-2022-21247
oracle -- essbase_administration_services	Vulnerability in the Oracle Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported version that is affected is Prior to 11.1.2.4.047. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Essbase Administration Services. While the vulnerability is in Oracle Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Essbase Administration Services. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2022-01-19	6.5	CVE-2021-35683
oracle -- financial_services_analytical_applications_infrastructure	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Unified Metadata Manager). Supported versions that are affected are 8.0.7-8.1.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure 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).	2022-01-19	5	CVE-2021-35687

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- financial_services_analytical_applications_infrastructure	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Unified Metadata Manager). Supported versions that are affected are 8.0.7-8.1.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure 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).	2022-01-19	4	CVE-2021-35686
oracle -- graalvm	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, 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 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2022-01-19	5	CVE-2022-21271
oracle -- graalvm	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, 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 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2022-01-19	5	CVE-2022-21277
oracle -- graalvm	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. 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).	2022-01-19	5	CVE-2022-21282
oracle -- graalvm	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle	2022-01-19	4.3	CVE-2022-21248

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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 Enterprise Edition accessible data. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. 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).			
oracle -- graalvm	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, 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 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2022-01-19	5	CVE-2022-21283
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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).	2022-01-19	6.8	CVE-2022-21253
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27 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).	2022-01-19	6.8	CVE-2022-21256
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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).	2022-01-19	4	CVE-2022-21264
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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).	2022-01-19	4	CVE-2022-21270

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.27 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	2022-01-19	5.5	CVE-2022-21301
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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 update, insert or delete access to some of MySQL Server 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).	2022-01-19	4	CVE-2022-21245
oracle -- mysql	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	2022-01-19	4	CVE-2022-21284
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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 update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L).	2022-01-19	5.5	CVE-2022-21265
oracle -- mysql	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	2022-01-19	4	CVE-2022-21285
oracle -- mysql	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	2022-01-19	4	CVE-2022-21286
oracle -- mysql	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows	2022-01-19	4	CVE-2022-21287

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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).	2022-01-19	6.3	CVE-2022-21254
oracle -- mysql	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	2022-01-19	4	CVE-2022-21288
oracle -- mysql	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	2022-01-19	4	CVE-2022-21289
oracle -- mysql	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	2022-01-19	4	CVE-2022-21290
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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).	2022-01-19	4	CVE-2022-21297
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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	2022-01-19	4	CVE-2022-21304

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(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 8.0.27 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2022-01-19	4	CVE-2022-21249
oracle -- peoplesoft_enterprise_cs_sa_integration_pack	Vulnerability in the PeopleSoft Enterprise CS SA Integration Pack product of Oracle PeopleSoft (component: Snapshot Integration). Supported versions that are affected are 9.0 and 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise CS SA Integration Pack. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS SA Integration Pack accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2022-01-19	5	CVE-2022-21300
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.57, 8.58 and 8.59. 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. 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).	2022-01-19	5.8	CVE-2022-21272
oracle -- primavera_portfolio_management	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0 and 20.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera Portfolio Management 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).	2022-01-19	5.8	CVE-2022-21269
oracle -- primavera_portfolio_management	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0 and 20.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Primavera Portfolio Management. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2022-01-19	4	CVE-2022-21243
oracle -- primavera_portfolio_management	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0 and 20.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via	2022-01-19	4.9	CVE-2022-21242

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera Portfolio 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).			
oracle -- primavera_portfolio_management	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0 and 20.0.0.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).	2022-01-19	4.9	CVE-2022-21281
oracle -- primavera_portfolio_management	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0 and 20.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	2022-01-19	4.3	CVE-2022-21244
oracle -- project_costing	Vulnerability in the Oracle Project Costing product of Oracle E-Business Suite (component: Expenses, Currency Override). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Project Costing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Project Costing accessible data as well as unauthorized access to critical data or complete access to all Oracle Project Costing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2022-01-19	5.5	CVE-2022-21273
oracle -- solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Fault Management Architecture). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data as well as unauthorized read access to a subset of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 4.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L).	2022-01-19	6	CVE-2022-21263
oracle -- trade_management	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: GL Accounts). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification	2022-01-19	5.5	CVE-2022-21250

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access to critical data or all Oracle Trade Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).			
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server 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).	2022-01-19	5.8	CVE-2022-21261
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2022-01-19	5	CVE-2022-21292
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server 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).	2022-01-19	5.8	CVE-2022-21259
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). The supported version that is affected is 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server 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).	2022-01-19	5.8	CVE-2022-21258
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic	2022-01-19	5.8	CVE-2022-21257

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Server 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).			
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server 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).	2022-01-19	5.8	CVE-2022-21260
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2022-01-19	6.4	CVE-2022-21252
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server 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).	2022-01-19	5.8	CVE-2022-21262
owncloud -- files_antivirus	The files_antivirus component before 1.0.0 for ownCloud mishandles the protection mechanism by which malicious files (that have been uploaded to a public share) are supposed to be deleted upon detection.	2022-01-15	6.5	CVE-2021-33828
owncloud -- owncloud	ownCloud owncloud/client before 2.9.2 allows Resource Injection by a server into the desktop client via a URL, leading to remote code execution.	2022-01-15	6.8	CVE-2021-44537
parity -- frontier	Frontier is Substrate's Ethereum compatibility layer. Prior to commit number `8a93fdc6c9f4eb1d2f2a11b7ff1d12d70bf5a664`, a bug in Frontier's MODEXP precompile implementation can cause an integer underflow in certain conditions. This will cause a node crash for debug builds. For release builds (and production WebAssembly binaries), the impact is limited as it can only cause a normal EVM out-of-gas. Users who do not use MODEXP precompile in their runtime are not impacted. A patch is available in pull request #549.	2022-01-14	4	CVE-2022-21685
pexip -- infinity	Pexip Infinity before 26 allows remote denial of service because of missing RTMP input validation.	2022-01-15	5	CVE-2021-32545
phoronix-media -- phoronix_test_suite	phoronix-test-suite is vulnerable to Cross-Site Request Forgery (CSRF)	2022-01-16	4.3	CVE-2022-0238
qnap -- qcalagent	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running QcalAgent. If exploited, this vulnerability allows remote attackers to inject	2022-01-14	4.3	CVE-2021-38677

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	malicious code. We have already fixed this vulnerability in the following versions of QcalAgent: QcalAgent 1.1.7 and later			
qnap -- qcalagent	An open redirect vulnerability has been reported to affect QNAP device running QcalAgent. If exploited, this vulnerability allows attackers to redirect users to an untrusted page that contains malware. We have already fixed this vulnerability in the following versions of QcalAgent: QcalAgent 1.1.7 and later	2022-01-14	5.8	CVE-2021-38678
ray-ban -- stories_rw4003_65582v_48-23_firmware	A logic flaw in Ray-Ban® Stories device software allowed some parameters like video capture duration limit to be modified through the Facebook View application. This issue affected versions of device software before 2107460.6810.0.	2022-01-14	5	CVE-2021-24046
ropium_project -- ropium	ROPium v3.1 was discovered to contain an invalid memory address dereference via the find() function.	2022-01-14	5	CVE-2021-45761
salonerp_project -- salonerp	In SalonERP 3.0.1, a SQL injection vulnerability allows an attacker to inject payload using 'sql' parameter in SQL query while generating a report. Upon successfully discovering the login admin password hash, it can be decrypted to obtain the plain-text password.	2022-01-14	6.5	CVE-2021-45406
samsung -- internet	Incorrect download source UI in Downloads in Samsung Internet prior to 16.0.6.23 allows attackers to perform domain spoofing via a crafted HTML page.	2022-01-14	4.3	CVE-2022-22290
sap -- enterprise_threat_detection	SAP Enterprise Threat Detection (ETD) - version 2.0, does not sufficiently encode user-controlled inputs which may lead to an unauthorized attacker possibly exploit XSS vulnerability. The UIs in ETD are using SAP UI5 standard controls, the UI5 framework provides automated output encoding for its standard controls. This output encoding prevents stored malicious user input from being executed when it is reflected in the UI.	2022-01-14	4.3	CVE-2022-22529
sap -- netweaver_abap	In SAP NetWeaver AS for ABAP and ABAP Platform - versions 701, 702, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 786, an attacker authenticated as a regular user can use the S/4 Hana dashboard to reveal systems and services which they would not normally be allowed to see. No information alteration or denial of service is possible.	2022-01-14	4	CVE-2021-42067
sap -- s\/4hana	The F0743 Create Single Payment application of SAP S/4HANA - versions 100, 101, 102, 103, 104, 105, 106, does not check uploaded or downloaded files. This allows an attacker with basic user rights to run arbitrary script code, resulting in sensitive information being disclosed or modified.	2022-01-14	5.5	CVE-2022-22531
spin_project -- spin	Spin v6.5.1 was discovered to contain an out-of-bounds write in lex() at spinlex.c.	2022-01-14	4.3	CVE-2021-46168
tenable -- tenable.sc	Tenable.sc versions 5.14.0 through 5.19.1 were found to contain a remote code execution vulnerability which could allow a remote, unauthenticated attacker to execute code under special circumstances. An attacker would first have to stage a specific file type in the web server root of the Tenable.sc host prior to remote exploitation.	2022-01-14	6.8	CVE-2022-0130
vim -- vim	vim is vulnerable to Heap-based Buffer Overflow	2022-01-14	6.8	CVE-2022-0213 MLIST
we-con -- levistudiou	WECON LeviStudioU Versions 2019-09-21 and prior are vulnerable to a heap-based buffer overflow, which may allow an attacker to remotely execute code.	2022-01-14	6.8	CVE-2021-23157
we-con -- levistudiou	WECON LeviStudioU Versions 2019-09-21 and prior are vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute code.	2022-01-14	6.8	CVE-2021-23138

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accu-time -- maximus_firmware	Accu-Time Systems MAXIMUS 1.0 telnet service suffers from a remote buffer overflow which causes the telnet service to crash	2022-01-10	5	CVE-2021-45856
adobe -- experience_manager	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a reflected Cross-Site Scripting (XSS) vulnerability via the itemResourceType parameter. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser	2022-01-13	4.3	CVE-2021-44178
adobe -- experience_manager	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2022-01-13	4.3	CVE-2021-43765
adobe -- experience_manager	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2022-01-13	4.3	CVE-2021-44177
adobe -- experience_manager	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2022-01-13	4.3	CVE-2021-44176
adobe -- incopy	Adobe InCopy version 16.4 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-13	6.8	CVE-2021-45055
adobe -- incopy	Adobe InCopy version 16.4 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-13	6.8	CVE-2021-45056
adobe -- incopy	Adobe InCopy version 16.4 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-13	6.8	CVE-2021-45053
adobe -- incopy	Adobe InCopy version 16.4 (and earlier) is affected by a use-after-free vulnerability in the processing of a JPEG2000 file that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2022-01-13	4.3	CVE-2021-45054
adobe -- indesign	Adobe InDesign version 16.4 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious JPEG file.	2022-01-13	6.8	CVE-2021-45058
adobe -- indesign	Adobe InDesign version 16.4 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious JPEG2000 file.	2022-01-13	6.8	CVE-2021-45057
adobe -- indesign	Adobe InDesign version 16.4 (and earlier) is affected by a use-after-free vulnerability in the processing of a JPEG2000 file that could lead to disclosure of	2022-01-13	4.3	CVE-2021-45059

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
apache -- guacamole	Apache Guacamole 1.3.0 and older may incorrectly include a private tunnel identifier in the non-private details of some REST responses. This may allow an authenticated user who already has permission to access a particular connection to read from or interact with another user's active use of that same connection.	2022-01-11	4	CVE-2021-41767 MLIST
apache -- guacamole	Apache Guacamole 1.2.0 and 1.3.0 do not properly validate responses received from a SAML identity provider. If SAML support is enabled, this may allow a malicious user to assume the identity of another Guacamole user.	2022-01-11	6	CVE-2021-43999 MLIST
atlassian -- data_center	Affected versions of Atlassian Jira Service Management Server and Data Center allow authenticated remote attackers to view object import configuration details via an Information Disclosure vulnerability in the Create Object type mapping feature. The affected versions are before version 4.21.0.	2022-01-10	4	CVE-2021-43951
atlassian -- data_center	Affected versions of Atlassian Jira Service Management Server and Data Center allow authenticated remote attackers to view private objects via a Broken Access Control vulnerability in the Custom Fields feature. The affected versions are before version 4.21.0.	2022-01-10	4	CVE-2021-43949
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of DGN files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14883.	2022-01-13	4.3	CVE-2021-34910
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14865.	2022-01-13	6.8	CVE-2021-34898
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of 3DS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14862.	2022-01-13	6.8	CVE-2021-34895
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of BMP files. 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-14863.	2022-01-13	6.8	CVE-2021-34896
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction	2022-01-13	4.3	CVE-2021-34944

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15052.			
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15051.	2022-01-13	4.3	CVE-2021-34943
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14894.	2022-01-13	4.3	CVE-2021-34916
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14828.	2022-01-13	6.8	CVE-2021-34876
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of BMP files. 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-14695.	2022-01-13	6.8	CVE-2021-34871
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of SKP files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14737.	2022-01-13	6.8	CVE-2021-34872
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of PDF files. Crafted data in a PDF file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14696.	2022-01-13	6.8	CVE-2021-34873
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 processing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14736.	2022-01-13	6.8	CVE-2021-34874

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of 3DS files. Crafted data in a 3DS file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14827.	2022-01-13	6.8	CVE-2021-34875
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of DGN files. Crafted data in a DGN file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14864.	2022-01-13	6.8	CVE-2021-34897
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14830.	2022-01-13	6.8	CVE-2021-34878
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14900.	2022-01-13	6.8	CVE-2021-34922
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14885.	2022-01-13	6.8	CVE-2021-34912
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of DGN files. Crafted data in a DGN file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14892.	2022-01-13	6.8	CVE-2021-34914
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14899.	2022-01-13	6.8	CVE-2021-34921
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the	2022-01-13	6.8	CVE-2021-34909

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14882.			
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of J2K files. 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-14867.	2022-01-13	6.8	CVE-2021-34900
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of BMP files. Crafted data in a BMP file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14876.	2022-01-13	6.8	CVE-2021-34903
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of DGN files. 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-14877.	2022-01-13	6.8	CVE-2021-34904
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of DGN files. 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-14878.	2022-01-13	6.8	CVE-2021-34905
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of J2K files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14879.	2022-01-13	6.8	CVE-2021-34906
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of BMP files. 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-14880.	2022-01-13	6.8	CVE-2021-34907
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of J2K files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14881.	2022-01-13	6.8	CVE-2021-34908
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. User interaction is required to exploit this	2022-01-13	6.8	CVE-2021-34911

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14884.			
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14898.	2022-01-13	6.8	CVE-2021-34920
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14838.	2022-01-13	6.8	CVE-2021-34885
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14831.	2022-01-13	6.8	CVE-2021-34913
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14866.	2022-01-13	6.8	CVE-2021-34899
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of J2K files. Crafted data in a J2K file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14893.	2022-01-13	6.8	CVE-2021-34915
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of J2K files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14895.	2022-01-13	6.8	CVE-2021-34917
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JP2 files. Crafted data in a JP2 file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14896.	2022-01-13	6.8	CVE-2021-34918

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JP2 files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14897.	2022-01-13	6.8	CVE-2021-34919
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of 3DS files. Crafted data in a 3DS file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14833.	2022-01-13	6.8	CVE-2021-34880
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of J2K files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14832.	2022-01-13	6.8	CVE-2021-34879
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14844.	2022-01-13	6.8	CVE-2021-34891
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15039.	2022-01-13	6.8	CVE-2021-34940
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15040.	2022-01-13	6.8	CVE-2021-34941
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14842.	2022-01-13	4.3	CVE-2021-34889
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack	2022-01-13	6.8	CVE-2021-34939

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14996.			
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14905.	2022-01-13	6.8	CVE-2021-34927
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14906.	2022-01-13	6.8	CVE-2021-34928
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14907.	2022-01-13	6.8	CVE-2021-34929
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14845.	2022-01-13	6.8	CVE-2021-34892
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14910.	2022-01-13	6.8	CVE-2021-34932
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. 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-15054.	2022-01-13	6.8	CVE-2021-34945
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14911.	2022-01-13	6.8	CVE-2021-34933

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14909.	2022-01-13	6.8	CVE-2021-34931
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14913.	2022-01-13	6.8	CVE-2021-34935
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14914.	2022-01-13	6.8	CVE-2021-34936
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14915.	2022-01-13	6.8	CVE-2021-34937
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. 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-14995.	2022-01-13	6.8	CVE-2021-34938
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14912.	2022-01-13	6.8	CVE-2021-34934
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15041.	2022-01-13	6.8	CVE-2021-34942
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this	2022-01-13	6.8	CVE-2021-34930

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability to execute code in the context of the current process. Was ZDI-CAN-14908.			
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15055.	2022-01-13	6.8	CVE-2021-34946
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of JP2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14835.	2022-01-13	4.3	CVE-2021-34882
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of BMP files. 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-14846.	2022-01-13	6.8	CVE-2021-34893
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of 3DS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14847.	2022-01-13	6.8	CVE-2021-34894
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14829.	2022-01-13	6.8	CVE-2021-34877
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14901.	2022-01-13	6.8	CVE-2021-34923
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14903.	2022-01-13	6.8	CVE-2021-34925

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14904.	2022-01-13	6.8	CVE-2021-34926
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of OBJ files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14834.	2022-01-13	4.3	CVE-2021-34881
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of J2K files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14836.	2022-01-13	4.3	CVE-2021-34883
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14875.	2022-01-13	4.3	CVE-2021-34902
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of JP2 files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14837.	2022-01-13	4.3	CVE-2021-34884
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of FBX files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14839.	2022-01-13	4.3	CVE-2021-34886
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in	2022-01-13	4.3	CVE-2021-34887

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14840.			
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14841.	2022-01-13	4.3	CVE-2021-34888
bentley -- bentley_view	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14902.	2022-01-13	6.8	CVE-2021-34924
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14843.	2022-01-13	4.3	CVE-2021-34890
bentley -- bentley_view	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 parsing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14874.	2022-01-13	4.3	CVE-2021-34901
daybydaycrm -- daybyday	In DayByDay CRM, versions 2.2.0 through 2.2.1 (latest) are vulnerable to Insufficient Session Expiration. When a password has been changed by the user or by an administrator, a user that was already logged in, will still have access to the application even after the password was changed.	2022-01-13	5.5	CVE-2022-22113
dst-admin_project -- dst-admin	An issue was discovered in dst-admin v1.3.0. The product has an unauthorized arbitrary file download vulnerability that can expose sensitive information.	2022-01-10	5	CVE-2021-44586
fastlinemedia -- beaver_builder	In Beaver Builder through 2.5.0.3, attackers can bypass the visibility controls protection mechanism via the REST API.	2022-01-10	5	CVE-2021-42748
fastlinemedia -- beaver_themer	In Beaver Themer, attackers can bypass conditional logic controls (for hiding content) when viewing the post archives. Exploitation requires that a Themer layout is applied to the archives, and that the post excerpt field is not set.	2022-01-10	5	CVE-2021-42749
framasoft -- peertube	peertube is vulnerable to Improper Access Control	2022-01-10	5	CVE-2022-0133
framasoft -- peertube	peertube is vulnerable to Server-Side Request Forgery (SSRF)	2022-01-10	5	CVE-2022-0132
google -- android	An improper check or handling of exceptional conditions in NPU driver prior to SMR Jan-2022 Release 1 allows arbitrary memory write and code execution.	2022-01-10	4.6	CVE-2022-22265

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In showCarrierAppInstallationNotification of EuiccNotificationManager.java, there is a possible way to gain an access to MediaProvider content due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-9Android ID: A-194695347	2022-01-14	6.9	CVE-2021-39625
google -- android	An implicit Intent hijacking vulnerability in Dialer prior to SMR Jan-2022 Release 1 allows unprivileged applications to access contact information.	2022-01-10	4.3	CVE-2022-22270
google -- google-protobuf	An issue in protobuf-java allowed the interleaving of com.google.protobuf.UnknownFieldSet fields in such a way that would be processed out of order. A small malicious payload can occupy the parser for several minutes by creating large numbers of short-lived objects that cause frequent, repeated pauses. We recommend upgrading libraries beyond the vulnerable versions.	2022-01-10	4.3	CVE-2021-22569 MLIST MLIST
gpac -- gpac	A Pointer Dereference Vulnerability exists in GPAC 1.0.1 via the gf_fileio_check function, which could cause a Denial of Service.	2022-01-10	4.3	CVE-2021-46049
gpac -- gpac	A buffer overflow vulnerability exists in Gpac through 1.0.1 via a malformed MP4 file in the svc_parse_slice function in av_parsers.c, which allows attackers to cause a denial of service, even code execution and escalation of privileges.	2022-01-13	6.8	CVE-2021-40568
gpac -- gpac	The binary MP4Box in Gpac 1.0.1 has a null pointer dereference vulnerability in the mpgviddmx_process function in reframe_mpgvid.c, which allows attackers to cause a denial of service. This vulnerability is possibly due to an incomplete fix for CVE-2021-40566.	2022-01-13	4.3	CVE-2021-40575
gpac -- gpac	A Pointer Dereference Vulnerability exists in GPAC 1.0.1 via the Media_IsSelfContained function, which could cause a Denial of Service. .	2022-01-10	4.3	CVE-2021-46051
gpac -- gpac	A Pointer Derefernce Vulnerbility exists GPAC 1.0.1 the gf_isom_box_size function, which could cause a Denial of Service (context-dependent).	2022-01-10	4.3	CVE-2021-46046
gpac -- gpac	A Pointer Dereference Vulnerability exists in GPAC 1.0.1 via the gf_hinter_finalize function.	2022-01-10	4.3	CVE-2021-46047
gpac -- gpac	The binary MP4Box in Gpac 1.0.1 has a double-free bug in the av1dmx_finalize function in reframe_av1.c, which allows attackers to cause a denial of service.	2022-01-13	4.3	CVE-2021-40572
gpac -- gpac	The binary MP4Box in Gpac 1.0.1 has a null pointer dereference vulnerability in the gf_isom_get_payt_count function in hint_track.c, which allows attackers to cause a denial of service.	2022-01-13	4.3	CVE-2021-40576
gpac -- gpac	GPAC 1.0.1 is affected by: Abort failed. The impact is: cause a denial of service (context-dependent).	2022-01-10	4.3	CVE-2021-46045
gpac -- gpac	The binary MP4Box in Gpac 1.0.1 has a double-free vulnerability in the gf_list_del function in list.c, which allows attackers to cause a denial of service.	2022-01-13	4.3	CVE-2021-40573
gpac -- gpac	The binary MP4Box in Gpac 1.0.1 has a double-free vulnerability in the gf_text_get_utf8_line function in load_text.c, which allows attackers to cause a denial of service, even code execution and escalation of privileges.	2022-01-13	6.8	CVE-2021-40574
gpac -- gpac	The binary MP4Box in Gpac through 1.0.1 has a double-free vulnerability in the iloc_entry_del funciton in box_code_meta.c, which allows attackers to cause a denial of service.	2022-01-13	4.3	CVE-2021-40569
gpac -- gpac	A Segmentation fault casued by heap use after free vulnerability exists in Gpac through 1.0.1 via the mpgviddmx_process function in reframe_mpgvid.c when using mp4box, which causes a denial of service.	2022-01-12	4.3	CVE-2021-40566

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac -- gpac	A Segmentation fault caused by a null pointer dereference vulnerability exists in Gpac through 1.0.1 via the gf_avc_parse_nalu function in av_parsers.c when using mp4box, which causes a denial of service.	2022-01-12	4.3	CVE-2021-40565
gpac -- gpac	A Segmentation fault caused by null pointer dereference vulnerability eists in Gpac through 1.0.2 via the avc_parse_slice function in av_parsers.c when using mp4box, which causes a denial of service.	2022-01-12	4.3	CVE-2021-40564
gpac -- gpac	A Segmentation fault exists casued by null pointer dereference exists in Gpac through 1.0.1 via the naludmx_create_avc_decoder_config function in reframe_nalu.c when using mp4box, which causes a denial of service.	2022-01-12	4.3	CVE-2021-40563
gpac -- gpac	A Segmentation fault caused by a floating point exception exists in Gpac through 1.0.1 using mp4box via the naludmx_enqueue_or_dispatch function in reframe_nalu.c, which causes a denial of service.	2022-01-12	4.3	CVE-2021-40562
gpac -- gpac	A null pointer deference vulnerability exists in gpac through 1.0.1 via the naludmx_parse_nal_avc function in reframe_nalu, which allows a denail of service.	2022-01-12	4.3	CVE-2021-40559
gpac -- gpac	The binary MP4Box in Gpac 1.0.1 has a double-free vulnerability in the ilst_box_read function in box_code_apple.c, which allows attackers to cause a denial of service, even code execution and escalation of privileges.	2022-01-13	6.8	CVE-2021-40571
gpac -- gpac	The binary MP4Box in Gpac 1.0.1 has a double-free vulnerability in the avc_compute_poc function in av_parsers.c, which allows attackers to cause a denial of service, even code execution and escalation of privileges.	2022-01-13	6.8	CVE-2021-40570
gpac -- gpac	A heap-based buffer overflow vulnerability exists in GPAC v1.0.1 in the gf_isom_dovi_config_get function in MP4Box, which causes a denial of service or execute arbitrary code via a crafted file.	2022-01-12	6.8	CVE-2021-36417
gpac -- gpac	Segmentation fault vulnerability exists in Gpac through 1.0.1 via the gf_odf_size_descriptor function in desc_private.c when using mp4box, which causes a denial of service.	2022-01-13	4.3	CVE-2021-40567
htmldoc_project -- htmldoc	A stack-based buffer overflow in image_load_bmp() in HTMLDOC <= 1.9.13 results in remote code execution if the victim converts an HTML document linking to a crafted BMP file.	2022-01-10	6.8	CVE-2021-43579
huawei -- emui	There is a Null pointer dereference vulnerability in the camera module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	2022-01-10	5	CVE-2021-40031
huawei -- emui	There is an Out-of-bounds array read vulnerability in the security storage module in smartphones. Successful exploitation of this vulnerability may affect service confidentiality.	2022-01-10	5	CVE-2021-40020
huawei -- emui	There is an Uncontrolled resource consumption vulnerability in the display module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	2022-01-10	6.4	CVE-2021-40011
huawei -- harmonyos	The bone voice ID TA has a vulnerability in information management,Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	5	CVE-2021-40032
huawei -- harmonyos	The Bluetooth module has an out-of-bounds write vulnerability. Successful exploitation of this vulnerability may result in malicious command execution at the remote end.	2022-01-10	5.8	CVE-2021-40000
huawei -- harmonyos	The eID module has an out-of-bounds memory write vulnerability,Successful exploitation of this vulnerability may affect data integrity.	2022-01-10	5	CVE-2021-40028
huawei -- harmonyos	The bone voice ID TA has a vulnerability in calculating the buffer length,Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	5	CVE-2021-40027

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- harmonyos	There is a Heap-based buffer overflow vulnerability in the AOD module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	2022-01-10	5	CVE-2021-40026
huawei -- harmonyos	The eID module has a vulnerability that causes the memory to be used without being initialized,Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	5	CVE-2021-40025
huawei -- harmonyos	The weaver module has a vulnerability in parameter type verification,Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	5	CVE-2021-40022
huawei -- harmonyos	There is an Out-of-bounds write vulnerability in the AOD module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	2022-01-10	5	CVE-2021-40009
huawei -- harmonyos	The eID module has an out-of-bounds memory write vulnerability,Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	5	CVE-2021-40021
huawei -- harmonyos	There is a Double free vulnerability in the AOD module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	2022-01-10	5	CVE-2021-40038
huawei -- harmonyos	There is a Buffer overflow vulnerability due to a boundary error with the Samba server in the file management module in smartphones. Successful exploitation of this vulnerability may affect function stability.	2022-01-10	5	CVE-2021-40029
huawei -- harmonyos	There is a Null pointer dereference vulnerability in the camera module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	2022-01-10	5	CVE-2021-40039
huawei -- harmonyos	There is a Buffer overflow vulnerability due to a boundary error with the Samba server in the file management module in smartphones. Successful exploitation of this vulnerability may affect function stability.	2022-01-10	5	CVE-2021-40035
huawei -- harmonyos	HwPCAssistant has a path traversal vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	5	CVE-2021-40003
huawei -- harmonyos	The distributed data service component has a vulnerability in data access control. Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	5	CVE-2021-40005
huawei -- harmonyos	The CaasKit module has a path traversal vulnerability. Successful exploitation of this vulnerability may cause the MeeTime application to be unavailable.	2022-01-10	5	CVE-2021-40001
huawei -- harmonyos	There is a Vulnerability of accessing resources using an incompatible type (type confusion) in the MPTCP subsystem in smartphones. Successful exploitation of this vulnerability may cause the system to crash and restart.	2022-01-10	4.9	CVE-2021-40037
huawei -- harmonyos	The bone voice ID trusted application (TA) has a heap overflow vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	5	CVE-2021-40014
huawei -- harmonyos	The cellular module has a vulnerability in permission management. Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	5	CVE-2021-40004
huawei -- harmonyos	The eID module has a null pointer reference vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	5	CVE-2021-40018
huawei -- harmonyos	The Bluetooth module has an out-of-bounds write vulnerability. Successful exploitation of this vulnerability may result in malicious command execution at the remote end.	2022-01-10	5.8	CVE-2021-40002
ibm -- security_verify_access	IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 could disclose sensitive information due to hazardous input validation during QR code generation. IBM X-Force ID: 212040.	2022-01-10	5	CVE-2021-38957 XF

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_access	IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 210067.	2022-01-10	5	CVE-2021-38921 XF
ibm -- security_verify_access	IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 could disclose sensitive version information in HTTP response headers that could aid in further attacks against the system. IBM X-Force ID: 212038	2022-01-10	5	CVE-2021-38956 XF
ibm -- security_verify_access	IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 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: 209515.	2022-01-10	4	CVE-2021-38894 XF
ibm -- vios	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the mount command which could lead to code execution. IBM X-Force ID: 212952.	2022-01-10	4.6	CVE-2021-38990 XF
kentico -- kentico_cms	Kentico Xperience 13.0.44 allows XSS via an XML document to the Media Libraries subsystem.	2022-01-10	4.3	CVE-2021-46163
kubernetes -- kubernetes	kubectl does not neutralize escape, meta or control sequences contained in the raw data it outputs to a terminal. This includes but is not limited to the unstructured string fields in objects such as Events.	2022-01-07	5.8	CVE-2021-25743
libexpat_project -- libexpat	lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	2022-01-10	6.8	CVE-2022-22825
libexpat_project -- libexpat	nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	2022-01-10	6.8	CVE-2022-22826
libexpat_project -- libexpat	storeAtts in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	2022-01-10	6.8	CVE-2022-22827
libmeshb_project -- libmeshb	A buffer overflow in the GmfOpenMesh() function of libMeshb v7.61 allows attackers to cause a Denial of Service (DoS) via a crafted MESH file.	2022-01-12	4.3	CVE-2021-46225
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. A denial of service (resource consumption) can be accomplished by searching for a very long key in a Language Name Search.	2022-01-10	5	CVE-2021-46149
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. MassEditRegex allows CSRF.	2022-01-10	6.8	CVE-2021-46147
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. Some unprivileged users can view confidential information (e.g., IP addresses and User-Agent headers for election traffic) on a testwiki SecurePoll instance.	2022-01-10	4	CVE-2021-46148
metagauss -- registrationmagic	The RegistrationMagic WordPress plugin before 5.0.1.6 does not escape user input in its rm_chronos_ajax AJAX action before using it in a SQL statement when duplicating tasks in batches, which could lead to a SQL injection issue	2022-01-10	6.5	CVE-2021-24862
microsoft -- excel	Microsoft Office Remote Code Execution Vulnerability.	2022-01-11	6.8	CVE-2022-21840
microsoft -- sharepoint_enterprise_server	Microsoft Word Remote Code Execution Vulnerability.	2022-01-11	6.8	CVE-2022-21842
microsoft -- windows_10	Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-21848, CVE-2022-21883, CVE-2022-21889, CVE-2022-21890.	2022-01-11	4.3	CVE-2022-21843
microsoft -- windows_10	Windows Push Notifications Apps Elevation Of Privilege Vulnerability.	2022-01-11	6.9	CVE-2022-21867

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Accounts Control Elevation of Privilege Vulnerability.	2022-01-11	6.9	CVE-2022-21859
microsoft -- windows_10	Windows Hyper-V Denial of Service Vulnerability.	2022-01-11	4.9	CVE-2022-21847
microsoft -- windows_10	Windows Devices Human Interface Elevation of Privilege Vulnerability.	2022-01-11	6.9	CVE-2022-21868
microsoft -- windows_10	Windows StateRepository API Server file Elevation of Privilege Vulnerability.	2022-01-11	6.9	CVE-2022-21863
microsoft -- windows_10	Windows Application Model Core API Elevation of Privilege Vulnerability.	2022-01-11	6.9	CVE-2022-21862
mitre -- caldera	An issue was discovered in CALDERA 2.9.0. The Debrief plugin receives base64 encoded "SVG" parameters when generating a PDF document. These SVG documents are parsed in an unsafe manner and can be leveraged for XXE attacks (e.g., File Exfiltration, Server Side Request Forgery, Out of Band Exfiltration, etc.).	2022-01-12	6.5	CVE-2021-42560
philips -- engage	The affected product is vulnerable to an improper access control, which may allow an authenticated user to gain unauthorized access to sensitive data.	2022-01-10	4	CVE-2021-23173
pluginus -- woocommerce_currency_switcher	The WOOCS WordPress plugin before 1.3.7.3 does not sanitise and escape the custom_prices parameter before outputting it back in the response, leading to a Reflected Cross-Site Scripting issue	2022-01-10	4.3	CVE-2021-25043
qnap -- qts	A cross-site scripting (XSS) vulnerability has been reported to affect QTS, QuTS hero and QuTScloud. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of QTS, QuTS hero and QuTScloud: QuTS hero h4.5.4.1771 build 20210825 and later QTS 4.5.4.1787 build 20210910 and later QuTScloud c4.5.7.1864 and later	2022-01-07	4.3	CVE-2021-38674
qualcomm -- apq8009w_firmware	Possible denial of service due to incorrectly decoding hex data for the SIB2 OTA message and assigning a garbage value to choice when processing the SRS configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	2022-01-13	5	CVE-2021-30300
qualcomm -- ar8031_firmware	Improper validation of memory region in Hypervisor can lead to incorrect region mapping in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2022-01-13	4.6	CVE-2021-30285
qualcomm -- ar8035_firmware	Possible assertion due to improper validation of symbols configured for PDCCH monitoring in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	2022-01-13	5	CVE-2021-30287
qualcomm -- ar8035_firmware	Possible denial of service due to improper validation of DNS response when DNS client requests with PTR, NAPTR or SRV query type in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT	2022-01-13	5	CVE-2021-30307
qualcomm -- ar8035_firmware	Possible denial of service due to out of memory while processing RRC and NAS OTA message in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon Mobile	2022-01-13	5	CVE-2021-30301
rubyonrails -- rails	A open redirect vulnerability exists in Action Pack >= 6.0.0 that could allow an attacker to craft a "X-Forwarded-Host" headers in combination with certain "allowed host" formats can cause the Host Authorization middleware in Action Pack to redirect users to a malicious website.	2022-01-10	5.8	CVE-2021-44528
siemens -- comos	A vulnerability has been identified in COMOS (All versions < V10.4.1). The COMOS Web component of COMOS uses a flawed implementation of CSRF prevention. An	2022-01-11	6.8	CVE-2021-37198

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker could exploit this vulnerability to perform Cross-Site-Request-Forgery attacks.			
siemens -- comos	A vulnerability has been identified in COMOS (All versions < V10.4.1). The COMOS Web component of COMOS unpacks specially crafted archive files to relative paths. This vulnerability could allow an attacker to store files in any folder accessible by the COMOS Web webservice.	2022-01-11	4	CVE-2021-37196
siemens -- comos	A vulnerability has been identified in COMOS (All versions < V10.4.1). The COMOS Web component of COMOS is vulnerable to SQL injections. This could allow an attacker to execute arbitrary SQL statements.	2022-01-11	6.5	CVE-2021-37197
siemens -- comos	A vulnerability has been identified in COMOS (All versions < V10.4.1). The COMOS Web component of COMOS accepts arbitrary code as attachment to tasks. This could allow an attacker to inject malicious code that is executed when loading the attachment.	2022-01-11	4.3	CVE-2021-37195
sismics -- teedy	In Teedy, versions v1.5 through v1.9 are vulnerable to Reflected Cross-Site Scripting (XSS). The “search term" search functionality is not sufficiently sanitized while displaying the results of the search, which can be leveraged to inject arbitrary scripts. These scripts are executed in a victim’s browser when they enter the crafted URL. In the worst case, the victim who inadvertently triggers the attack is a highly privileged administrator. The injected scripts can extract the Session ID, which can lead to full Account Takeover of the administrator, by an unauthenticated attacker.	2022-01-10	4.3	CVE-2022-22114
snipeitapp -- snipe-it	snipe-it is vulnerable to Improper Access Control	2022-01-12	4.9	CVE-2022-0179
soketi_project -- soketi	soketi is an open-source WebSockets server. There is an unhandled case when reading POST requests which results in the server crashing if it could not read the body of a request. In the event that a POST request is sent to any endpoint of the server with an empty body, even unauthenticated with the Pusher Protocol, it will crash the server. All users that run the server are affected by this vulnerability and it's highly recommended to upgrade to the latest patch. There are no workarounds for this issue.	2022-01-10	5	CVE-2022-21667
sphinxsearch -- sphinx	SphinxSearch in Sphinx Technologies Sphinx through 3.1.1 allows directory traversal (in conjunction with CVE-2019-14511) because the mysql client can be used for CALL SNIPPETS and load_file operations on a full pathname (e.g., a file in the /etc directory). NOTE: this is unrelated to CMUSphinx.	2022-01-10	5	CVE-2020-29050 MLIST
trendmicro -- apex_one	A link following denial-of-service vulnerability in Trend Micro Apex One (on-prem and SaaS) and Trend Micro Worry-Free Business Security (10.0 SP1 and Services) could allow a local attacker to overwrite arbitrary files in the context of SYSTEM. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2022-01-10	6.6	CVE-2021-44024
trendmicro -- apex_one	A link following denial-of-service vulnerability in Trend Micro Worry-Free Business Security (on prem only) could allow a local attacker to overwrite arbitrary files in the context of SYSTEM. This is similar to, but not the same as CVE-2021-44024. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2022-01-10	6.6	CVE-2021-45442
ultimaker -- ultimaker_s3_firmware	In Ultimaker S3 3D printer, Ultimaker S5 3D printer, Ultimaker 3 3D printer S-line through 6.3 and Ultimaker 3 through 5.2.16, the local webserver can be used for clickjacking. This includes the settings page.	2022-01-10	6.8	CVE-2021-34087
ultimaker -- ultimaker_s3_firmware	In Ultimaker S3 3D printer, Ultimaker S5 3D printer, Ultimaker 3 3D printer S-line through 6.3 and Ultimaker 3 through 5.2.16, the local webserver hosts APIs vulnerable to CSRF. They do not verify incoming requests.	2022-01-10	6.8	CVE-2021-34086

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vim -- vim	vim is vulnerable to Heap-based Buffer Overflow	2022-01-10	4.3	CVE-2022-0158 FEDORA MLIST
vim -- vim	vim is vulnerable to Use After Free	2022-01-10	4.3	CVE-2022-0156 FEDORA MLIST
vmware -- spring_framework	In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.	2022-01-10	4	CVE-2021-22060
webassembly -- binaryen	A Stack Overflow vulnerability exists in Binaryen 103 via the printf_common function.	2022-01-10	4.3	CVE-2021-46050
webassembly -- binaryen	A Denial of Service vulnerability exists in Binaryen 103. The program terminates with signal SIGKILL.	2022-01-10	4.3	CVE-2021-46053
webassembly -- binaryen	A Denial of Service vulnerability exists in Binaryen 104 due to an assertion abort in wasm::WasmBinaryBuilder::readFunctions.	2022-01-10	4.3	CVE-2021-46048
webassembly -- binaryen	A Denial of Service vulnerability exists in Binaryen 104 due to an assertion abort in wasm::Tuple::validate.	2022-01-10	4.3	CVE-2021-46052
webassembly -- binaryen	A Denial of Service vulnerability exists in Binaryen 104 due to an assertion abort in wasm::WasmBinaryBuilder::visitRethrow(wasm::Rethrow*).	2022-01-10	4.3	CVE-2021-46054
webassembly -- binaryen	A Denial of Service vulnerability exists in Binaryen 104 due to an assertion abort in wasm::WasmBinaryBuilder::visitRethrow(wasm::Rethrow*).	2022-01-10	4.3	CVE-2021-46055
wow-company -- button_generator	The Button Generator WordPress plugin before 2.3.3 within the wow-company admin menu page allows to include() arbitrary file with PHP extension (as well as with data:// or http:// protocols), thus leading to CSRF RCE.	2022-01-10	5.1	CVE-2021-25052
wow-company -- modal_window	The Modal Window WordPress plugin before 5.2.2 within the wow-company admin menu page allows to include() arbitrary file with PHP extension (as well as with data:// or http:// protocols), thus leading to CSRF RCE.	2022-01-10	5.1	CVE-2021-25051
wow-company -- wp_coder	The WP Coder WordPress plugin before 2.5.2 within the wow-company admin menu page allows to include() arbitrary file with PHP extension (as well as with data:// or http:// protocols), thus leading to CSRF RCE.	2022-01-10	5.1	CVE-2021-25053
wow-company -- wpcalc	The WPcalc WordPress plugin through 2.1 does not sanitize user input into the 'did' parameter and uses it in a SQL statement, leading to an authenticated SQL Injection vulnerability.	2022-01-10	6.5	CVE-2021-25054
zohocorp -- manageengine_desktop_central	Zoho ManageEngine Desktop Central before 10.0.662 allows remote code execution by an authenticated user who has complete access to the Reports module.	2022-01-10	6.5	CVE-2021-46164
zohocorp -- manageengine_desktop_central	Zoho ManageEngine Desktop Central before 10.0.662, during startup, launches an executable file from the batch files, but this file's path might not be properly defined.	2022-01-10	4.6	CVE-2021-46165
zohocorp -- manageengine_desktop_central	Zoho ManageEngine Desktop Central before 10.0.662 allows authenticated users to obtain sensitive information from the database by visiting the Reports page.	2022-01-10	4	CVE-2021-46166

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adtribes -- product_feed_pro_for_woocommerce	The Product Feed PRO for WooCommerce WordPress plugin before 11.0.7 does not have authorisation and CSRF check in some of its AJAX actions, allowing any authenticated users to call then, which could lead to Stored Cross-Site Scripting issue (which will be triggered in the admin dashboard) due to the lack of escaping.	2022-01-24	3.5	CVE-2021-24974
b3log -- vditor	Cross-site Scripting (XSS) - Stored in GitHub repository vanessa219/vditor prior to 1.0.34.	2022-01-23	3.5	CVE-2021-4103
dell -- emc_system_update	Dell EMC System Update, version 1.9.2 and prior, contain an Unprotected Storage of Credentials vulnerability. A local attacker with user privleges could potentially exploit this vulnerability leading to the disclosure of user passwords.	2022-01-24	2.1	CVE-2022-22554
etoilewebdesign -- ultimate_faq	The Ultimate FAQ WordPress plugin before 2.1.2 does not have capability and CSRF checks in the ewd_ufaq_welcome_add_faq and ewd_ufaq_welcome_add_faq_page AJAX actions, available to any authenticated users. As a result, any users, with a role as low as Subscriber could create FAQ and FAQ questions	2022-01-24	3.5	CVE-2021-24968
fivestarplugins -- five_star_restaurant_reservations	The Five Star Restaurant Reservations WordPress plugin before 2.4.8 does not have capability and CSRF checks in the rtb_welcome_set_schedule AJAX action, allowing any authenticated users to call it. Due to the lack of sanitisation and escaping, users with a role as low as subscriber could perform Cross-Site Scripting attacks against logged in admins	2022-01-24	3.5	CVE-2021-24965
fresenius-kabi -- agilia_connect	An attacker with physical access to the host can extract the secrets from the registry and create valid JWT tokens for the Fresenius Kabi Vigilant MasterMed version 2.0.1.3 application and impersonate arbitrary users. An attacker could manipulate RabbitMQ queues and messages by impersonating users.	2022-01-21	2.1	CVE-2021-23207
getgrav -- grav	Cross-site Scripting (XSS) - Stored in Packagist getgrav/grav prior to 1.7.28.	2022-01-25	3.5	CVE-2022-0268
graphql-go_project -- graphql-go	graphql-go is a GraphQL server with a focus on ease of use. In versions prior to 1.3.0 there exists a DoS vulnerability that is possible due to a bug in the library that would allow an attacker with specifically designed queries to cause stack overflow panics. Any user with access to the GraphQL handler can send these queries and cause stack overflows. This in turn could potentially compromise the ability of the server to serve data to its users. The issue has been patched in version `v1.3.0`. The only known workaround for this issue is to disable the `graphql.MaxDepth` option from your schema which is not recommended.	2022-01-21	3.5	CVE-2022-21708
iconics -- genesis64	Plaintext Storage of a Password vulnerability in Mitsubishi Electric MC Works64 versions 4.04E (10.95.210.01) and prior and ICONICS GENESIS64 versions 10.90 to 10.97 allows a local authenticated attacker to gain authentication information and to access the database illegally. This is because when configuration information of GridWorX, a database linkage function of GENESIS64 and MC Works64, is exported to a CSV file, the authentication information is saved in plaintext, and an attacker who can access this CSV file can gain the authentication information.	2022-01-21	2.1	CVE-2022-23129
jflyfox -- jfinal_cms	In jfinal_cms >= 5.1 0, there is a storage XSS vulnerability in the background system of CMS. Because developers do not filter the parameters submitted by the user input form, any user with background permission can affect the system security by entering malicious code.	2022-01-25	3.5	CVE-2021-46087
mobile_events_manager_project -- mobile_events_manager	The Mobile Events Manager WordPress plugin before 1.4.4 does not sanitise and escape various of its settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	2022-01-24	3.5	CVE-2021-25049
rapid7 -- insight_agent	Rapid7 Insight Agent, versions prior to 3.1.3, suffer from an improper access control vulnerability whereby, the user has access to the snapshot directory. An attacker can access, read and copy any of the files in this directory e.g.	2022-01-21	2.1	CVE-2021-4016

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	asset_info.json or file_info.json, leading to a loss of confidentiality. This issue was fixed in Rapid7 Insight Agent 3.1.3.			
showdoc -- showdoc	Cross-site Scripting (XSS) - Stored in GitHub repository star7th/showdoc prior to 2.10.2.	2022-01-22	3.5	CVE-2021-4172
spotweb_project -- spotweb	Cross site scripting (XSS) vulnerability in spotweb 1.4.9, allows authenticated attackers to execute arbitrary code via crafted GET request to the login page.	2022-01-21	3.5	CVE-2021-33966
student_quarterly_grading_system_project -- student_quarterly_grading_system	Cross Site Scripting (XSS) in Sourcecodester Student Quarterly Grading System by oretnom23, allows attackers to execute arbitrary code via the fullname and username parameters to the users page.	2022-01-24	3.5	CVE-2021-41658
tipsandtricks-hq -- simple_download_monitor	The Simple Download Monitor WordPress plugin before 3.9.11 could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attack via 1) "color" or "css_class" argument of sdm_download shortcode, 2) "class" or "placeholder" argument of sdm_search_form shortcode.	2022-01-24	3.5	CVE-2021-24694
updraftplus -- updraftplus	The UpdraftPlus WordPress Backup Plugin WordPress plugin before 1.6.59 does not sanitise its updraft_service settings, allowing high privilege users to set malicious JavaScript payload in it and leading to a Stored Cross-Site Scripting issue	2022-01-24	3.5	CVE-2021-24423
uscat_project -- uscat	uscat, as of 2021-12-28, is vulnerable to Cross Site Scripting (XSS) via the input box of the statistical code.	2022-01-25	3.5	CVE-2021-46083
uscat_project -- uscat	uscat, as of 2021-12-28, is vulnerable to Cross Site Scripting (XSS) via "close registration information" input box.	2022-01-25	3.5	CVE-2021-46084
wbolt -- smart_seo_tool	The Smart SEO Tool WordPress plugin before 3.0.6 does not sanitise and escape the search parameter before outputting it back in an attribute when the TDK optimisation setting is enabled, leading to a Reflected Cross-Site Scripting	2022-01-24	2.6	CVE-2021-24976
asus -- rt-ax56u_firmware	ASUS RT-AX56U’s login function contains a path traversal vulnerability due to its inadequate filtering for special characters in URL parameters, which allows an unauthenticated local area network attacker to access restricted system paths and download arbitrary files.	2022-01-14	3.3	CVE-2022-22054
calibre-web_project -- calibre-web	calibre-web is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2022-01-16	3.5	CVE-2021-4170
cisco -- ip_conference_phone_7832_firmware	A vulnerability in the information storage architecture of several Cisco IP Phone models could allow an unauthenticated, physical attacker to obtain confidential information from an affected device. This vulnerability is due to unencrypted storage of confidential information on an affected device. An attacker could exploit this vulnerability by physically extracting and accessing one of the flash memory chips. A successful exploit could allow the attacker to obtain confidential information from the device, which could be used for subsequent attacks.	2022-01-14	2.1	CVE-2022-20660 CISCO FULLDISC
google -- android	In gre_handle_offloads of ip_gre.c, there is a possible page fault due to an invalid memory access. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-150694665References: Upstream kernel	2022-01-14	2.1	CVE-2021-39633
google -- android	In sec_SHA256_Transform of sha256_core.c, there is a possible way to read heap data due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-197965864References: N/A	2022-01-14	2.1	CVE-2021-39680

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- sterling_gentran	IBM Sterling Gentran:Server for Microsoft Windows 5.3 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 213962.	2022-01-14	2.1	CVE-2021-39032 XF
nanoid_project -- nanoid	The package nanoid before 3.1.31 are vulnerable to Information Exposure via the valueOf() function which allows to reproduce the last id generated.	2022-01-14	2.1	CVE-2021-23566
opensuse -- factory	A Incorrect Default Permissions vulnerability in the parsec package of openSUSE Factory allows local attackers to imitate the service leading to DoS or clients talking to an imposter service. This issue affects: openSUSE Factory parsec versions prior to 0.8.1-1.1.	2022-01-14	3.6	CVE-2021-36781
oracle -- communications_billing_and_revenue_management	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Pipeline Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Communications Billing and Revenue Management executes to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Billing and Revenue Management accessible data. CVSS 3.1 Base Score 3.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2022-01-19	2.1	CVE-2022-21267
oracle -- communications_billing_and_revenue_management	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Pipeline Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Communications Billing and Revenue Management executes to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Billing and Revenue Management accessible data. CVSS 3.1 Base Score 3.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2022-01-19	2.1	CVE-2022-21268
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 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).	2022-01-19	3.5	CVE-2022-21302
oracle -- solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Install). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).	2022-01-19	3.3	CVE-2022-21298
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.32. Easily exploitable 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. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base	2022-01-19	2.1	CVE-2022-21295

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).			
sap -- business_one	SAP Business One - version 10.0, extended log stores information that can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.	2022-01-14	2.1	CVE-2021-44234
tribe29 -- checkmk	A stored cross site scripting (XSS) vulnerability in Checkmk 1.6.0x prior to 1.6.0p19 allows an authenticated remote attacker to inject arbitrary JavaScript via a javascript: URL in a view title.	2022-01-15	3.5	CVE-2020-28919
wpchill -- download_monitor	Authenticated Reflected Cross-Site Scripting (XSS) vulnerability discovered in WordPress plugin Download Monitor (versions <= 4.4.6).	2022-01-14	3.5	CVE-2021-36920
adobe -- experience_manager	AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2022-01-13	3.5	CVE-2021-43764
fit2cloud -- halo	In Halo, versions v1.0.0 to v1.4.17 (latest) are vulnerable to Stored Cross-Site Scripting (XSS) in the article title. An authenticated attacker can inject arbitrary javascript code that will execute on a victim's server.	2022-01-13	3.5	CVE-2022-22123
fit2cloud -- halo	In Halo, versions v1.0.0 to v1.4.17 (latest) are vulnerable to Stored Cross-Site Scripting (XSS) in the profile image. An authenticated attacker can upload a carefully crafted SVG file that will trigger arbitrary javascript to run on a victim's browser.	2022-01-13	3.5	CVE-2022-22124
google -- android	Unprotected dynamic receiver in SecSettings prior to SMR Jan-2022 Release 1 allows untrusted applications to launch arbitrary activity.	2022-01-10	2.1	CVE-2022-22263
google -- android	Improper sanitization of incoming intent in Dressroom prior to SMR Jan-2022 Release 1 allows local attackers to read and write arbitrary files without permission.	2022-01-10	3.6	CVE-2022-22264
google -- android	In StatusBar.java, there is a possible disclosure of notification content on the lockscreen due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-189575031	2022-01-14	2.1	CVE-2021-39628
google -- android	Incorrect implementation of Knox Guard prior to SMR Jan-2022 Release 1 allows physically proximate attackers to temporary unlock the Knox Guard via Samsung DeX mode.	2022-01-10	3.6	CVE-2022-22268
google -- android	(Applicable to China models only) Unprotected WifiEvaluationService in TencentWifiSecurity application prior to SMR Jan-2022 Release 1 allows untrusted applications to get WiFi information without proper permission.	2022-01-10	2.1	CVE-2022-22266
google -- android	Implicit Intent hijacking vulnerability in ActivityMetricsLogger prior to SMR Jan-2022 Release 1 allows attackers to get running application information.	2022-01-10	2.1	CVE-2022-22267
google -- android	Keeping sensitive data in unprotected BluetoothSettingsProvider prior to SMR Jan-2022 Release 1 allows untrusted applications to get a local Bluetooth MAC address.	2022-01-10	2.1	CVE-2022-22269
google -- android	A missing input validation before memory copy in TIMA trustlet prior to SMR Jan-2022 Release 1 allows attackers to copy data from arbitrary memory.	2022-01-10	2.1	CVE-2022-22271
google -- android	Improper authorization in TelephonyManager prior to SMR Jan-2022 Release 1 allows attackers to get IMSI without READ_PRIVILEGED_PHONE_STATE permission	2022-01-10	2.1	CVE-2022-22272

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- harmonyos	The fingerprint module has a security risk of brute force cracking. Successful exploitation of this vulnerability may affect data confidentiality.	2022-01-10	2.1	CVE-2021-40006
huawei -- ws318n-21_firmware	There is a Cross-Site Scripting(XSS) vulnerability in HUAWEI WS318n product when processing network settings. Due to insufficient validation of user input, a local authenticated attacker could exploit this vulnerability by injecting special characters. Successful exploit could cause certain information disclosure. Affected product versions include: WS318n-21 10.0.2.2, 10.0.2.5 and 10.0.2.6.	2022-01-10	1.9	CVE-2021-40041
ibm -- security_verify_access	IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 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: 209563.	2022-01-10	3.5	CVE-2021-38895 XF
ivanti -- workspace_control	A insecure storage of sensitive information vulnerability exists in Ivanti Workspace Control <2021.2 (10.7.30.0) that could allow an attacker with locally authenticated low privileges to obtain key information due to an unspecified attack vector.	2022-01-10	2.1	CVE-2022-21823
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. Special:CheckUserLog allows CheckUser XSS because of date mishandling, as demonstrated by an XSS payload in MediaWiki:October.	2022-01-10	3.5	CVE-2021-46150
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. The WikibaseMediaInfo component is vulnerable to XSS via the caption fields for a given media file.	2022-01-10	3.5	CVE-2021-46146
microsoft -- windows_10	Windows Event Tracing Discretionary Access Control List Denial of Service Vulnerability.	2022-01-11	2.1	CVE-2022-21839
phoronix-media -- phoronix_test_suite	phoronix-test-suite is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2022-01-10	3.5	CVE-2022-0157
rangerstudio -- directus	In Directus, versions 9.0.0-alpha.4 through 9.4.1 allow unrestricted file upload of .html files in the media upload functionality, which leads to Cross-Site Scripting vulnerability. A low privileged attacker can upload a crafted HTML file as a profile avatar, and when an admin or another user opens it, the XSS payload gets triggered.	2022-01-10	3.5	CVE-2022-22117
rangerstudio -- directus	In Directus, versions 9.0.0-alpha.4 through 9.4.1 are vulnerable to stored Cross-Site Scripting (XSS) vulnerability via SVG file upload in media upload functionality. A low privileged attacker can inject arbitrary javascript code which will be executed in a victim's browser when they open the image URL.	2022-01-10	3.5	CVE-2022-22116
sismics -- teedy	In Teedy, versions v1.5 through v1.9 are vulnerable to Stored Cross-Site Scripting (XSS) in the name of a created Tag. Since the Tag name is not being sanitized properly in the edit tag page, a low privileged attacker can store malicious scripts in the name of the Tag. In the worst case, the victim who inadvertently triggers the attack is a highly privileged administrator. The injected scripts can extract the Session ID, which can lead to full Account Takeover of the administrator, and privileges escalation.	2022-01-10	3.5	CVE-2022-22115