BULLETIN (SB21-242)

VULNERABILITY SUMMARY FOR THE WEEK OF

23RD AUGUST, 2021

Bulletin (SB21-242)
Vulnerability Summary for the Week of August 23, 2021

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.
The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

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

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .
The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- bridge	Adobe Bridge version 11.0.2 (and earlier) are affected by a Heap-based Buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	9.3	CVE-2021-28624
adobe -- bridge	Adobe Bridge version 11.0.2 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	9.3	CVE-2021-35989
adobe -- bridge	Adobe Bridge version 11.0.2 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	9.3	CVE-2021-35990
adobe -- illustrator	Adobe Illustrator version 25.2.3 (and earlier) is affected by an memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	9.3	CVE-2021-36009
adobe -- illustrator	Adobe Illustrator version 25.2.3 (and earlier) is affected by a potential Command injection vulnerability when chained with a development and debugging tool for JavaScript scripts. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	9.3	CVE-2021-36011
adobe -- media_encoder	Adobe Media Encoder version 15.2 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	9.3	CVE-2021-36015
altus -- nexto_nx3003_firmware	Authenticated Semi-Blind Command Injection (via Parameter Injection) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via the getlogs.cgi tcpdump feature. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0.	2021-08-23	9	CVE-2021-39244
att -- xmill	A heap-based buffer overflow vulnerability exists in the XML Decompression DecodeTreeBlock functionality of AT&T Labs Xmill 0.7. Within `DecodeTreeBlock` which is called during the decompression of an XMI file, a UINT32 is loaded from the file and used as trusted input as the length of a buffer. An attacker can provide a malicious file to trigger this vulnerability.	2021-08-20	7.5	CVE-2021-21826
att -- xmill	A heap-based buffer overflow vulnerability exists in the XML Decompression DecodeTreeBlock functionality of AT&T Labs Xmill 0.7. Within `DecodeTreeBlock` which is called during the decompression of an XMI file, a UINT32 is loaded from the file and used as trusted input as the length of a buffer. An attacker can provide a malicious file to trigger this vulnerability.	2021-08-20	7.5	CVE-2021-21827
att -- xmill	A heap-based buffer overflow vulnerability exists in the XML Decompression DecodeTreeBlock functionality of AT&T Labs Xmill 0.7. In the default case of DecodeTreeBlock a label is created via CurPath::AddLabel in order to track the label for later reference. An attacker can provide a malicious file to trigger this vulnerability.	2021-08-20	7.5	CVE-2021-21828
bludit -- bludit	Unrestricted File Upload in Bludit v3.8.1 allows remote attackers to execute arbitrary code by uploading malicious files via the component 'bl-kereln/ajax/upload-logo.php'.	2021-08-20	7.5	CVE-2020-18879
edit_comments_project -- edit_comments	The Edit Comments WordPress plugin through 0.3 does not sanitise, validate or escape the jal_edit_comments GET parameter before using it in a SQL statement, leading to a SQL injection issue	2021-08-23	7.5	CVE-2021-24551
netmodule -- nb800_firmware	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800.	2021-08-23	7.5	CVE-2021-39290
nuishop -- nuishop	Nuishop v2.3 contains a SQL injection vulnerability in /goods/getGoodsListByConditions/.	2021-08-26	7.5	CVE-2020-20675

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
safecurl_project -- safecurl	SafeCurl before 0.9.2 has a DNS rebinding vulnerability.	2021-08-20	7.5	CVE-2020-36474
cisco -- application_extension_platform	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability.	2021-08-18	10	CVE-2021-34730 CISCO
dated_news_project -- dated_news	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 allows SQL Injection.	2021-08-13	7.5	CVE-2021-36789
throughtek -- kalay_p2p_software_development_kit	ThroughTek's Kalay Platform 2.0 network allows an attacker to impersonate an arbitrary ThroughTek (TUTK) device given a valid 20-byte uniquely assigned identifier (UID). This could result in an attacker hijacking a victim's connection and forcing them into supplying credentials needed to access the victim TUTK device.	2021-08-17	7.6	CVE-2021-28372
alg_ds_project -- alg_ds	An issue was discovered in the alg_ds crate through 2020-08-25 for Rust. There is a drop of uninitialized memory in Matrix::new().	2021-08-08	7.5	CVE-2020-36432
care2x -- hospital_information_management_system	SQL Injection Vulnerability in Care2x Open Source Hospital Information Management 2.7 Alpha via the (1) pday, (2) pmonth, and (3) pyear parameters in GET requests sent to /modules/nursing/nursing-station.php.	2021-08-06	7.5	CVE-2021-36351
dell -- openmanage_enterprise	Dell OpenManage Enterprise versions prior to 3.6.1 contain an improper authentication vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to hijack an elevated session or perform unauthorized actions by sending malformed data.	2021-08-09	7.5	CVE-2021-21564 CONFIRM
dell -- openmanage_enterprise	Dell OpenManage Enterprise versions prior to 3.6.1 contain an OS command injection vulnerability in RACADM and IPMI tools. A remote authenticated malicious user with high privileges may potentially exploit this vulnerability to execute arbitrary OS commands.	2021-08-09	9	CVE-2021-21585 CONFIRM
dlink -- dir-615_firmware	A buffer overflow in D-Link DIR-615 C2 3.03WW. The ping_ipaddr parameter in ping_response.cgi POST request allows an attacker to crash the webserver and might even gain remote code execution.	2021-08-06	7.5	CVE-2021-37388
dreamsecurity -- magicline4nx.exe	A vulnerability in PKI Security Solution of Dream Security could allow arbitrary command execution. This vulnerability is due to insufficient validation of the authorization certificate. An attacker could exploit this vulnerability by sending a crafted HTTP request an affected program. A successful exploit could allow the attacker to remotely execute arbitrary code on a target system.	2021-08-06	10	CVE-2021-26606
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows memory corruption during conversion of a PDF document to a different document format.	2021-08-11	7.5	CVE-2021-38568
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows SQL Injection via crafted data at the end of a string.	2021-08-11	7.5	CVE-2021-38574
foxitsoftware -- foxit_reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write because the Cross-Reference table is mishandled during Office document conversion.	2021-08-11	7.5	CVE-2021-33793
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows writing to arbitrary files because a CombineFiles pathname is not validated.	2021-08-11	7.5	CVE-2021-38573
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows writing to arbitrary files because the extractPages pathname is not validated.	2021-08-11	7.5	CVE-2021-38572
gestionaleamica -- amica_prodigy	A vulnerability was found in CIR 2000 / Gestionale Amica Prodigy v1.7. The Amica Prodigy's executable "RemoteBackup.Service.exe" has incorrect permissions, allowing a local unprivileged user to replace it with a malicious file that will be executed with "LocalSystem" privileges.	2021-08-06	7.2	CVE-2021-35312
jeecg -- jeecg_boot	An arbitrary file upload vulnerability in /jeecg-boot/sys/common/upload of jeecg-boot CMS 2.3 allows attackers to execute arbitrary code.	2021-08-06	7.5	CVE-2020-28088
jetbrains -- hub	In JetBrains Hub before 2021.1.13389, account takeover was possible during password reset.	2021-08-06	7.5	CVE-2021-36209
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.4, there was an insecure deserialization.	2021-08-06	7.5	CVE-2021-37544
linux -- linux_kernel	In drivers/char/virtio_console.c in the Linux kernel before 5.13.4, data corruption or loss can be triggered by an untrusted device that supplies a buf->len value exceeding the buffer size.	2021-08-07	7.2	CVE-2021-38160

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
obsdian -- obsidian	Obsidian before 0.12.12 does not require user confirmation for non-http/https URLs.	2021-08-07	7.5	CVE-2021-38148
progress -- moveit_transfer	In certain Progress MOVEit Transfer versions before 2021.0.4 (aka 13.0.4), SQL injection in the MOVEit Transfer web application could allow an unauthenticated remote attacker to gain access to the database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, or execute SQL statements that alter or delete database elements, via crafted strings sent to unique MOVEit Transfer transaction types. The fixed versions are 2019.0.8 (11.0.8), 2019.1.7 (11.1.7), 2019.2.4 (11.2.4), 2020.0.7 (12.0.7), 2020.1.6 (12.1.6), and 2021.0.4 (13.0.4).	2021-08-07	7.5	CVE-2021-38159 CONFIRM
prolink -- prc2402m_firmware	In ProLink PRC2402M V1.0.18 and older, the set_sys_cmd function in the adm.cgi binary, accessible with a page parameter value of sysCMD contains a trivial command injection where the value of the command parameter is passed directly to system.	2021-08-06	7.5	CVE-2021-36706
prolink -- prc2402m_firmware	In ProLink PRC2402M V1.0.18 and older, the set_TR069 function in the adm.cgi binary, accessible with a page parameter value of TR069 contains a trivial command injection where the value of the TR069_local_port parameter is passed directly to system.	2021-08-06	7.5	CVE-2021-36705
prolink -- prc2402m_firmware	In ProLink PRC2402M V1.0.18 and older, the set_ledonoff function in the adm.cgi binary, accessible with a page parameter value of ledonoff contains a trivial command injection where the value of the led_cmd parameter is passed directly to do_system.	2021-08-06	7.5	CVE-2021-36707
rconfig -- rconfig	rConfig 3.9.5 allows command injection by sending a crafted GET request to lib/ajaxHandlers/ajaxArchiveFiles.php since the path parameter is passed directly to the exec function without being escaped.	2021-08-09	7.5	CVE-2020-23151
roxy-wi -- roxy-wi	Roxy-WI through 5.2.2.0 allows SQL Injection via check_login. An unauthenticated attacker can extract a valid uuid to bypass authentication.	2021-08-07	7.5	CVE-2021-38167
sys-info_project -- sys-info	An issue was discovered in the sys-info crate before 0.8.0 for Rust. sys_info::disk_info calls can trigger a double free.	2021-08-08	7.5	CVE-2020-36434

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aceide_project -- aceide	The AceIDE WordPress plugin through 2.6.2 does not sanitise or validate the user input which is appended to system paths before using it in various actions, such as to read arbitrary files from the server. This allows high privilege users such as administrator to access any file on the web server outside of the blog directory via a path traversal attack.	2021-08-23	4	CVE-2021-24549
adobe -- acrobat_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by a Type Confusion vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-08-20	4.3	CVE-2021-28643
adobe -- acrobat_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Use-after-free vulnerability. An authenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	6	CVE-2021-28640
adobe -- acrobat_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Use-after-free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	6.8	CVE-2021-28641
adobe -- acrobat_dc	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by an Out-of-bounds write vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	6.8	CVE-2021-28642
adobe -- bridge	Adobe Bridge version 11.0.2 (and earlier) is affected by an uninitialized variable vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-08-20	4.3	CVE-2021-35991
adobe -- bridge	Adobe Bridge version 11.0.2 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-08-20	4.3	CVE-2021-35992
adobe -- illustrator	Adobe Illustrator version 25.2.3 (and earlier) is affected by an Use-after-free vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to read arbitrary file system information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-08-20	4.3	CVE-2021-36008
adobe -- illustrator	Adobe Illustrator version 25.2.3 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	6.8	CVE-2021-28591
adobe -- illustrator	Adobe Illustrator version 25.2.3 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	6.8	CVE-2021-28592

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- illustrator	Adobe Illustrator version 25.2.3 (and earlier) is affected by a Use After Free vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose potential sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-08-20	4.3	CVE-2021-28593
adobe -- illustrator	Adobe Illustrator version 25.2.3 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of 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.	2021-08-20	4.3	CVE-2021-36010
adobe -- media_encoder	Adobe Media Encoder version 15.2 (and earlier) is affected by an uninitialized pointer vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to read arbitrary file system information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-08-20	4.3	CVE-2021-36014
adobe -- media_encoder	Adobe Media Encoder version 15.2 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to read arbitrary file system information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-08-20	4.3	CVE-2021-36016
adobe -- media_encoder	Adobe Media Encoder version 15.2 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	6.8	CVE-2021-28590
adobe -- media_encoder	Adobe Media Encoder version 15.2 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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.	2021-08-20	6.8	CVE-2021-28589
altus -- nexto_nx3003_firmware	Cross-Site Request Forgery (CSRF) exists on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices via any CGI endpoint. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0.	2021-08-23	4.3	CVE-2021-39243
altus -- nexto_nx3003_firmware	Hardcoded .htaccess Credentials for getlogs.cgi exist on Altus Nexto, Nexto Xpress, and Hadron Xtorm devices. This affects Nexto NX3003 1.8.11.0, Nexto NX3004 1.8.11.0, Nexto NX3005 1.8.11.0, Nexto NX3010 1.8.3.0, Nexto NX3020 1.8.3.0, Nexto NX3030 1.8.3.0, Nexto NX5100 1.8.11.0, Nexto NX5101 1.8.11.0, Nexto NX5110 1.1.2.8, Nexto NX5210 1.1.2.8, Nexto Xpress XP300 1.8.11.0, Nexto Xpress XP315 1.8.11.0, Nexto Xpress XP325 1.8.11.0, Nexto Xpress XP340 1.8.11.0, and Hadron Xtorm HX3040 1.7.58.0.	2021-08-23	5	CVE-2021-39245
arm -- mbed_tls	An issue was discovered in Mbed TLS before 2.24.0. The verification of X.509 certificates when matching the expected common name (the cn argument of mbedtls_x509_crt_verify) with the actual certificate name is mishandled: when the subjecAltName extension is present, the expected name is compared to any name in that extension regardless of its type. This means that an attacker could impersonate a 4-byte or 16-byte domain by getting a certificate for the corresponding IPv4 or IPv6 address (this would require the attacker to control that IP address, though).	2021-08-23	4.3	CVE-2020-36477
arm -- mbed_tls	An issue was discovered in Mbed TLS before 2.25.0 (and before 2.16.9 LTS and before 2.7.18 LTS). A NULL algorithm parameters entry looks identical to an array	2021-08-23	5	CVE-2020-36478

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of REAL (size zero) and thus the certificate is considered valid. However, if the parameters do not match in any way, then the certificate should be considered invalid.			
arm -- mbed_tls	An issue was discovered in Mbed TLS before 2.24.0 (and before 2.16.8 LTS and before 2.7.17 LTS). There is missing zeroization of plaintext buffers in mbedtls_ssl_read to erase unused application data from memory.	2021-08-23	5	CVE-2020-36476
arm -- mbed_tls	An issue was discovered in Mbed TLS before 2.25.0 (and before 2.16.9 LTS and before 2.7.18 LTS). The calculations performed by mbedtls_mpi_exp_mod are not limited; thus, supplying overly large parameters could lead to denial of service when generating Diffie-Hellman key pairs.	2021-08-23	5	CVE-2020-36475
broken_link_manager_project -- broken_link_manager	The Broken Link Manager WordPress plugin through 0.6.5 does not sanitise, validate or escape the url GET parameter before using it in a SQL statement when retrieving an URL to edit, leading to an authenticated SQL injection issue	2021-08-23	6.5	CVE-2021-24550
canon -- oce_print_exec_workgroup	Canon Oce Print Exec Workgroup 1.3.2 allows XSS via the lang parameter.	2021-08-23	4.3	CVE-2021-39368
contact_form_7_captcha_project -- contact_form_7_captcha	The Contact Form 7 Captcha WordPress plugin before 0.0.9 does not have any CSRF check in place when saving its settings, allowing attacker to make a logged in user with the manage_options change them. Furthermore, the settings are not escaped when output in attributes, leading to a Stored Cross-Site Scripting issue.	2021-08-23	6.8	CVE-2021-24565 CONFIRM
digitaldruid -- hoteldruid	DigitalDruid HotelDruid 3.0.2 has an XSS vulnerability in prenota.php affecting the fineperiodo1 parameter.	2021-08-26	4.3	CVE-2021-38559
eclipse -- californium	In Eclipse Californium version 2.0.0 to 2.6.4 and 3.0.0-M1 to 3.0.0-M3, the certificate based (x509 and RPK) DTLS handshakes accidentally succeeds without verifying the server side's signature on the client side, if that signature is not included in the server's ServerKeyExchange.	2021-08-20	5	CVE-2021-34433 CONFIRM
email-subscriber_project -- email-subscriber	The kento_email_subscriber_ajax AJAX action of the Email Subscriber WordPress plugin through 1.1, does not properly sanitise, validate and escape the submitted subscribe_email and subscribe_name POST parameters, inserting them in the DB and then outputting them back in the Subscriber list (/wp-admin/edit.php?post_type=kes_campaign&page=kento_email_subscriber_list_settings), leading a Stored XSS issue.	2021-08-23	4.3	CVE-2021-24556
f-secure -- atlant	A Denial-of-Service (DoS) vulnerability was discovered in all versions of F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine.	2021-08-23	4	CVE-2021-33598
firefly-iii -- firefly_iii	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF)	2021-08-23	4.3	CVE-2021-3730 CONFIRM
firefly-iii -- firefly_iii	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF)	2021-08-23	4.3	CVE-2021-3728 CONFIRM
firefly-iii -- firefly_iii	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF)	2021-08-23	4.3	CVE-2021-3729 CONFIRM
freelancetoindia -- paytm-pay	The Paytm â€“ Donation Plugin WordPress plugin through 1.3.2 does not sanitise, validate or escape the id GET parameter before using it in a SQL statement when deleting donations, leading to an authenticated SQL injection issue	2021-08-23	6.5	CVE-2021-24554

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
github -- owslib	An XML external entity (XXE) injection in PyWPS before 4.5.0 allows an attacker to view files on the application server filesystem by assigning a path to the entity. OWSLib 0.24.1 may also be affected.	2021-08-23	5	CVE-2021-39371
gitlab -- gitlab	Improper validation of invited users' email address in GitLab EE affecting all versions since 12.2 allowed projects to add members with email address domain that should be blocked by group settings	2021-08-23	4	CVE-2021-22251 CONFIRM
gitlab -- gitlab	A verbose error message in GitLab EE affecting all versions since 12.2 could disclose the private email address of a user invited to a group	2021-08-23	4	CVE-2021-22249 CONFIRM
gitlab -- gitlab	A vulnerability was discovered in GitLab versions before 14.0.2, 13.12.6, 13.11.6. GitLab Webhook feature could be abused to perform denial of service attacks.	2021-08-20	4	CVE-2021-22246 CONFIRM
gitlab -- gitlab	Improper authorization on the pipelines page in GitLab CE/EE affecting all versions since 13.12 allowed unauthorized users to view some pipeline information for public projects that have access to pipelines restricted to members only	2021-08-23	5	CVE-2021-22248 CONFIRM
gnome -- libgda	In GNOME libgda through 6.0.0, gda-web-provider.c does not enable TLS certificate verification on the SoupSessionSync objects it creates, leaving users vulnerable to network MITM attacks. NOTE: this is similar to CVE-2016-20011.	2021-08-22	4.3	CVE-2021-39359
gnome -- libgfbgraph	In GNOME libgfbgraph through 0.2.4, gfbgraph-photo.c does not enable TLS certificate verification on the SoupSessionSync objects it creates, leaving users vulnerable to network MITM attacks. NOTE: this is similar to CVE-2016-20011.	2021-08-22	4.3	CVE-2021-39358
google -- chrome	Use after free in WebRTC in Google Chrome prior to 92.0.4515.159 allowed an attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30602
google -- chrome	Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30598
google -- chrome	Use after free in Browser UI in Google Chrome on Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via physical access to the device.	2021-08-26	4.6	CVE-2021-30597
google -- chrome	Incorrect security UI in Navigation in Google Chrome on Android prior to 92.0.4515.131 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2021-08-26	4.3	CVE-2021-30596
google -- chrome	Use after free in Extensions API in Google Chrome prior to 92.0.4515.159 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30601
google -- chrome	Use after free in File System API in Google Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30591
google -- chrome	Out of bounds write in Tab Groups in Google Chrome prior to 92.0.4515.131 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30592
google -- chrome	Data race in WebAudio in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-08-26	5.1	CVE-2021-30603
google -- chrome	Out of bounds read in Tab Strip in Google Chrome prior to 92.0.4515.131 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted HTML page.	2021-08-26	5.8	CVE-2021-30593
google -- chrome	Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30599

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Use after free in Printing in Google Chrome prior to 92.0.4515.159 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30600
google -- chrome	Use after free in ANGLE in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30604
google -- chrome	Heap buffer overflow in Bookmarks in Google Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30590
google -- chrome	Use after free in Page Info UI in Google Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via physical access to the device.	2021-08-26	4.6	CVE-2021-30594
hmplugin -- hm_multiple_roles	The HM Multiple Roles WordPress plugin before 1.3 does not have any access control to prevent low privilege users to set themselves as admin via their profile page	2021-08-23	6.5	CVE-2021-24602
hucart -- hucart	SQL Injection vulnerability in Hucart CMS 5.7.4 via the basic information field found in the avatar usd_image field.	2021-08-26	6.5	CVE-2020-18476
hucart -- hucart	SQL Injection vulnerability in Hucart CMS 5.7.4 via the purchase enquiry field found in the Message con_content field.	2021-08-26	6.5	CVE-2020-18477
ibm -- resilient_security_orchestration_automation_and_response	IBM Security SOAR uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	2021-08-23	5	CVE-2021-29704 XF CONFIRM
ibm -- resilient_security_orchestration_automation_and_response	IBM Security SOAR performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses.	2021-08-23	5	CVE-2021-29802 XF CONFIRM
komoot -- komoot	An information disclosure vulnerability exists in the Friend finder functionality of GmbH Komoot version 10.26.9 up to 11.1.11. A specially crafted series of network requests can lead to the disclosure of sensitive information.	2021-08-20	5	CVE-2021-21823
ledgersmb -- ledgersmb	LedgerSMB does not sufficiently guard against being wrapped by other sites, making it vulnerable to 'clickjacking'. This allows an attacker to trick a targetted user to execute unintended actions.	2021-08-23	4.3	CVE-2021-3731 CONFIRM CONFIRM DEBIAN
ledgersmb -- ledgersmb	LedgerSMB does not sufficiently HTML-encode error messages sent to the browser. By sending a specially crafted URL to an authenticated user, this flaw can be abused for remote code execution and information disclosure.	2021-08-23	6.8	CVE-2021-3694 CONFIRM DEBIAN
ledgersmb -- ledgersmb	LedgerSMB does not check the origin of HTML fragments merged into the browser's DOM. By sending a specially crafted URL to an authenticated user, this flaw can be abused for remote code execution and information disclosure.	2021-08-23	6.8	CVE-2021-3693 CONFIRM DEBIAN
lifterlms -- lifterlms	The LMS by LifterLMS â€“ Online Course, Membership & Learning Management System Plugin for WordPress plugin before 4.21.2 was affected by an IDOR issue, allowing students to see other student answers and grades	2021-08-23	5	CVE-2021-24562

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netmodule -- nb800_firmware	Certain NetModule devices have Insecure Password Handling (cleartext or reversible encryption), These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800.	2021-08-23	5	CVE-2021-39289 CONFIRM
netmodule -- nb800_firmware	Certain NetModule devices allow credentials via GET parameters to CLI-PHP. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800.	2021-08-23	6.5	CVE-2021-39291
openstack -- neutron	OpenStack Neutron before 16.4.1, 17.x before 17.1.3, and 18.0.0 allows hardware address impersonation when the linuxbridge driver with ebtables-nft is used on a Netfilter-based platform. By sending carefully crafted packets, anyone in control of a server instance connected to the virtual switch can impersonate the hardware addresses of other systems on the network, resulting in denial of service or in some cases possibly interception of traffic intended for other destinations.	2021-08-23	5.8	CVE-2021-38598
phpmywind -- phpmywind	Unrestricted File Upload in PHPMyWind v5.6 allows remote attackers to execute arbitrary code via the component 'admin/upload_file_do.php'.	2021-08-20	6.5	CVE-2020-18886
phpmywind -- phpmywind	Command Injection in PHPMyWind v5.6 allows remote attackers to execute arbitrary code via the "text color" field of the component '/admin/web_config.php'.	2021-08-20	6.5	CVE-2020-18885
quantumcloud -- slider_hero	The Slider Hero with Animation, Video Background & Intro Maker WordPress plugin before 8.2.7 does not sanitise or escape the id attribute of its hero-button shortcode before using it in a SQL statement, allowing users with a role as low as Contributor to perform SQL injection.	2021-08-23	6.5	CVE-2021-24506
rconfig -- rconfig	An information disclosure vulnerability in rConfig 3.9.5 has been fixed for version 3.9.6. This vulnerability allowed remote authenticated attackers to read files on the system via a crafted request sent to to the /lib/crud/configcompare.crud.php script.	2021-08-20	4	CVE-2020-25351
rconfig -- rconfig	A server-side request forgery (SSRF) vulnerability in rConfig 3.9.5 has been fixed for 3.9.6. This vulnerability allowed remote authenticated attackers to open a connection to the machine via the deviceIpAddr and connPort parameters.	2021-08-20	4	CVE-2020-25353
rconfig -- rconfig	An insecure update feature in the /updater.php component of rConfig 3.9.6 and below allows attackers to execute arbitrary code via a crafted ZIP file.	2021-08-20	6.8	CVE-2020-27464
rconfig -- rconfig	An arbitrary file deletion vulnerability in rConfig 3.9.5 has been fixed for 3.9.6. This vulnerability gave attackers the ability to send a crafted request to /lib/ajaxHandlers/ajaxDeleteAllLoggingFiles.php by specifying a path in the path parameter and an extension in the ext parameter and delete all the files with that extension in that path.	2021-08-20	6.4	CVE-2020-25359
rconfig -- rconfig	An arbitrary file write vulnerability in lib/AjaxHandlers/ajaxEditTemplate.php of rConfig 3.9.6 allows attackers to execute arbitrary code via a crafted file.	2021-08-20	6.8	CVE-2020-27466
roosty -- diary-availability-calendar	The daac_delete_booking_callback function, hooked to the daac_delete_booking AJAX action, takes the id POST parameter which is passed into the SQL statement without proper sanitisation, validation or escaping, leading to a SQL Injection issue. Furthermore, the ajax action is lacking any CSRF and capability check, making it available to any authenticated user.	2021-08-23	6.5	CVE-2021-24555
simple_events_calendar_project -- simple_events_calendar	The Simple Events Calendar WordPress plugin through 1.4.0 does not sanitise, validate or escape the event_id POST parameter before using it in a SQL statement when deleting events, leading to an authenticated SQL injection issue	2021-08-23	6.5	CVE-2021-24552

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
skycaiji -- skycaiji	Directory Traversal in Skycaiji v1.3 allows remote attackers to obtain sensitive information via the component 'index.php?m=admin&c=Tool&a=log&file=D%3A%5CphpStudy%5CWWW%5Cindex.php'.	2021-08-20	5	CVE-2020-18878
timeline_calendar_project -- timeline_calendar	The Timeline Calendar WordPress plugin through 1.2 does not sanitise, validate or escape the edit GET parameter before using it in a SQL statement when editing events, leading to an authenticated SQL injection issue. Other SQL Injections are also present in the plugin	2021-08-23	6.5	CVE-2021-24553
totolink -- a3002r_firmware	Directory Indexing in Login Portal of Login Portal of TOTOLINK-A702R-V1.0.0-B20161227.1023 allows attacker to access /add/ , /img/, /js/, and /mobile directories via GET Parameter.	2021-08-20	5	CVE-2021-34218
totolink -- a3002r_firmware	Cross-site scripting in ddns.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "Domain Name" field, "Server Address" field, "User Name/Email", or "Password/Key" field.	2021-08-20	4.3	CVE-2021-34207
totolink -- a3002r_firmware	Cross-site scripting in tcpipwan.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "Service Name" field.	2021-08-20	4.3	CVE-2021-34215
totolink -- a3002r_firmware	Cross-site scripting in urlfilter.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "URL Address" field.	2021-08-20	4.3	CVE-2021-34223
totolink -- a3002r_firmware	Cross-site scripting in tr069config.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "User Name" field or "Password" field.	2021-08-20	4.3	CVE-2021-34220
totolink -- a3002r_firmware	Cross-site scripting in parent_control.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attackers to execute arbitrary JavaScript by modifying the "Description" field and "Service Name" field.	2021-08-20	4.3	CVE-2021-34228
wuzhicms -- wuzhicms	SQL Injection in Wuzhi CMS v4.1.0 allows remote attackers to obtain sensitive information via the 'flag' parameter in the component '/coreframe/app/order/admin/index.php'.	2021-08-20	5	CVE-2020-18877
xstream_project -- xstream	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.	2021-08-23	6	CVE-2021-39146 CONFIRM
xstream_project -- xstream	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.	2021-08-23	6	CVE-2021-39145 CONFIRM
xstream_project -- xstream	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker has sufficient rights to execute commands of the host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.	2021-08-23	6.5	CVE-2021-39144 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xstream_project -- xstream	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.	2021-08-23	6.5	CVE-2021-39141 CONFIRM
xstream_project -- xstream	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. A user is only affected if using the version out of the box with JDK 1.7u21 or below. However, this scenario can be adjusted easily to an external Xalan that works regardless of the version of the Java runtime. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.	2021-08-23	6.5	CVE-2021-39139 CONFIRM
dated_news_project -- dated_news	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 has incorrect Access Control for confirming various applications.	2021-08-13	6.4	CVE-2021-36792
dated_news_project -- dated_news	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 allows Information Disclosure of application registration data.	2021-08-13	5	CVE-2021-36791 CONFIRM
dated_news_project -- dated_news	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 allows XSS.	2021-08-13	4.3	CVE-2021-36790
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. In affected versions when running shape functions, some functions (such as `MutableHashTableShape`) produce extra output information in the form of a `ShapeAndType` struct. The shapes embedded in this struct are owned by an inference context that is cleaned up almost immediately; if the upstream code attempts to access this shape information, it can trigger a segfault. `ShapeRefiner` is mitigating this for normal output shapes by cloning them (and thus putting the newly created shape under ownership of an inference context that will not die), but we were not doing the same for shapes and types. This commit fixes that by doing similar logic on output shapes and types. We have patched the issue in GitHub commit ee119d4a498979525046fba1c3dd3f13a039fbb1. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.	2021-08-13	4.6	CVE-2021-37690 CONFIRM
routes_project -- routes	The routes (aka Extbase Yaml Routes) extension before 2.1.1 for TYPO3, when CsrfTokenViewHelper is used, allows Sensitive Information Disclosure because a session identifier is unsafely present in HTML output.	2021-08-13	5	CVE-2021-36793 CONFIRM
comrak_project -- comrak	An issue was discovered in the comrak crate before 0.10.1 for Rust. It mishandles & characters, leading to XSS via &# HTML entities.	2021-08-08	4.3	CVE-2021-38186
corero -- securewatch_managed_services	Corero SecureWatch Managed Services 9.7.2.0020 is affected by a Path Traversal vulnerability via the snap_file parameter in the /it-IT/splunkd/__raw/services/get_snapshot HTTP API endpoint. A ‘low privileged’ attacker can read any file on the target host.	2021-08-06	4	CVE-2021-38136
corero -- securewatch_managed_services	Corero SecureWatch Managed Services 9.7.2.0020 does not correctly check swa-monitor and cns-monitor user’s privileges, allowing a user to perform actions not belonging to his role.	2021-08-06	5.5	CVE-2021-38137
ctparental_project -- ctparental	CTparental before 4.45.03 is vulnerable to cross-site scripting (XSS) in the CTparental admin panel. In bl_categires_help.php, the 'categories' variable is	2021-08-10	4.3	CVE-2021-37365

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	assigned with the content of the query string param 'cat' without sanitization or encoding, enabling an attacker to inject malicious code into the output webpage.			
ctparental_project -- ctparental	CTparental before 4.45.03 is vulnerable to cross-site request forgery (CSRF) in the CTparental admin panel. By combining CSRF with XSS, an attacker can trick the administrator into clicking a link that cancels the filtering for all standard users.	2021-08-10	6.8	CVE-2021-37366
ctparental_project -- ctparental	CTparental before 4.45.07 is affected by a code execution vulnerability in the CTparental admin panel. Because The file "bl_categories_help.php" is vulnerable to directory traversal, an attacker can create a file that contains scripts and run arbitrary commands.	2021-08-10	4.6	CVE-2021-37367
dell -- openmanage_enterprise	Dell OpenManage Enterprise version 3.5 and OpenManage Enterprise-Modular version 1.30.00 contain an information disclosure vulnerability. An authenticated low privileged attacker may potentially exploit this vulnerability leading to disclosure of the OIDC server credentials.	2021-08-09	4	CVE-2021-21584 CONFIRM
dell -- openmanage_enterprise	Dell OpenManage Enterprise versions 3.4 through 3.6.1 and Dell OpenManage Enterprise Modular versions 1.20.00 through 1.30.00, contain a remote code execution vulnerability. A malicious attacker with access to the immediate subnet may potentially exploit this vulnerability leading to information disclosure and a possible elevation of privileges.	2021-08-09	5.8	CVE-2021-21596 CONFIRM
fig2dev_project -- fig2dev	A stack-based buffer overflow in the genptk_text component in genptk.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into ptk format.	2021-08-10	4.3	CVE-2020-21675
fortinet -- fortianalyzer	An improper access control vulnerability in FortiManager and FortiAnalyzer GUI interface 7.0.0, 6.4.5 and below, 6.2.8 and below, 6.0.11and below, 5.6.11and below may allow a remote and authenticated attacker with restricted user profile to retrieve the list of administrative users of other ADOMs and their related configuration.	2021-08-06	4	CVE-2021-32587 CONFIRM
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows attackers to delete arbitrary files (during uninstallation) via a symlink.	2021-08-11	6.4	CVE-2021-38570
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows DLL hijacking, aka CNVD-C-2021-68000 and CNVD-C-2021-68502.	2021-08-11	4.4	CVE-2021-38571
foxitsoftware -- foxit_reader	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows stack consumption via recursive function calls during the handling of XFA forms or link objects.	2021-08-11	5	CVE-2021-38569
foxitsoftware -- foxit_reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 allow information disclosure or an application crash after mishandling the Tab key during XFA form interaction.	2021-08-11	6.4	CVE-2021-33794
ignitedcms_project -- ignitedcms	Cross Site Request Forgery (CSRF) in IgnitedCMS v1.0 allows remote attackers to obtain sensitive information and gain privilege via the component "/admin/profile/save_profile".	2021-08-06	6.8	CVE-2020-18694
intelliants -- subrion	Cross-Site Scripting (XSS) vulnerability in Subrion 4.2.1 via the title when adding a page.	2021-08-06	4.3	CVE-2020-22330
jeecg -- jeecg_boot	A SQL injection vulnerability in /jeecg boot/sys/dict/loadtreedata of jeecg-boot CMS 2.3 allows attackers to access sensitive database information.	2021-08-06	5	CVE-2020-28087
jetbrains -- hub	In JetBrains Hub before 2021.1.13402, HTML injection in the password reset email was possible.	2021-08-06	4.3	CVE-2021-37541
jetbrains -- hub	In JetBrains Hub before 2021.1.13262, a potentially insufficient CSP for the Widget deployment feature was used.	2021-08-06	6.4	CVE-2021-37540

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- rubymine	In JetBrains RubyMine before 2021.1.1, code execution without user confirmation was possible for untrusted projects.	2021-08-06	6.5	CVE-2021-37543
jetbrains -- teamcity	In JetBrains TeamCity before 2021.1, passwords in cleartext sometimes could be stored in VCS.	2021-08-06	5	CVE-2021-37548
jetbrains -- teamcity	In JetBrains TeamCity before 2021.1, an insecure key generation mechanism for encrypted properties was used.	2021-08-06	5	CVE-2021-37546
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.3, XSS was possible.	2021-08-06	4.3	CVE-2021-37542
jetbrains -- teamcity	In JetBrains TeamCity before 2020.2.4, insufficient checks during file uploading were made.	2021-08-06	5	CVE-2021-37547
jetbrains -- teamcity	In JetBrains TeamCity before 2021.1.1, insufficient authentication checks for agent requests were made.	2021-08-06	5	CVE-2021-37545
jetbrains -- youtrack	In JetBrains YouTrack before 2021.3.21051, a user could see boards without having corresponding permissions.	2021-08-06	4	CVE-2021-37554
jetbrains -- youtrack	In JetBrains YouTrack before 2021.2.16363, an insecure PRNG was used.	2021-08-06	5	CVE-2021-37553
jetbrains -- youtrack	In JetBrains YouTrack before 2021.2.16363, system user passwords were hashed with SHA-256.	2021-08-06	5	CVE-2021-37551
jetbrains -- youtrack	In JetBrains YouTrack before 2021.2.16363, time-unsafe comparisons were used.	2021-08-06	5	CVE-2021-37550
jetbrains -- youtrack	In JetBrains YouTrack before 2021.1.11111, sandboxing in workflows was insufficient.	2021-08-06	6.4	CVE-2021-37549
leostream -- connection_broker	** UNSUPPORTED WHEN ASSIGNED ** LeoStream Connection Broker 9.x before 9.0.34.3 allows Unauthenticated Reflected XSS via the /index.pl user parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-08-06	4.3	CVE-2021-38157
linux -- linux_kernel	fs/nfsd/trace.h in the Linux kernel before 5.13.4 might allow remote attackers to cause a denial of service (out-of-bounds read in strlen) by sending NFS traffic when the trace event framework is being used for nfsd.	2021-08-08	5	CVE-2021-38202
linux -- linux_kernel	In kernel/bpf/hashtab.c in the Linux kernel through 5.13.8, there is an integer overflow and out-of-bounds write when many elements are placed in a single bucket. NOTE: exploitation might be impractical without the CAP_SYS_ADMIN capability.	2021-08-07	4.6	CVE-2021-38166
linux -- linux_kernel	fs/nfs/nfs4client.c in the Linux kernel before 5.13.4 has incorrect connection-setup ordering, which allows operators of remote NFSv4 servers to cause a denial of service (hanging of mounts) by arranging for those servers to be unreachable during trunking detection.	2021-08-08	5	CVE-2021-38199
linux -- linux_kernel	net/sunrpc/xdr.c in the Linux kernel before 5.13.4 allows remote attackers to cause a denial of service (xdr_set_page_base slab-out-of-bounds access) by performing many NFS 4.2 READ_PLUS operations.	2021-08-08	5	CVE-2021-38201
linux -- linux_kernel	drivers/net/ethernet/xilinx/ll_temac_main.c in the Linux kernel before 5.12.13 allows remote attackers to cause a denial of service (buffer overflow and lockup) by sending heavy network traffic for about ten minutes.	2021-08-08	5	CVE-2021-38207
lynx_project -- lynx	Lynx through 2.8.9 mishandles the userinfo subcomponent of a URI, which allows remote attackers to discover cleartext credentials because they may appear in SNI data.	2021-08-07	5	CVE-2021-38165

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MLIST MLIST MLIST MLIST DEBIAN
naviwebs -- navigate_cms	SQL Injection vulnerability in Naviwebs Navigate CMS 2.9 via the quicksearch parameter in \lib\packages\comments\comments.php.	2021-08-06	6.5	CVE-2021-36455
netapp -- cloud_manager	NetApp Cloud Manager versions prior to 3.9.9 log sensitive information when an Active Directory connection fails. The logged information is available only to authenticated users. Customers with auto-upgrade enabled should already be on a fixed version while customers using on-prem connectors with auto-upgrade disabled are advised to upgrade to a fixed version.	2021-08-06	4	CVE-2021-26999
netapp -- cloud_manager	NetApp Cloud Manager versions prior to 3.9.9 log sensitive information that is available only to authenticated users. Customers with auto-upgrade enabled should already be on a fixed version while customers using on-prem connectors with auto-upgrade disabled are advised to upgrade to a fixed version.	2021-08-06	4	CVE-2021-26998
popojicms -- popojicms	A stored cross site scripting (XSS) vulnerability in /admin.php?mod=user&act=addnew of PopojiCMS 1.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the E-Mail field.	2021-08-06	4.3	CVE-2020-21357
popojicms -- popojicms	An information disclosure vulnerability in upload.php of PopojiCMS 1.2 leads to physical path disclosure of the host when 'name = "file" is deleted during file uploads.	2021-08-06	5	CVE-2020-21356
project -- convec	An issue was discovered in the convec crate through 2020-11-24 for Rust. There are unconditional implementations of Send and Sync for ConVec<T>.	2021-08-08	6.8	CVE-2020-36445
prolink -- prc2402m_firmware	In ProLink PRC2402M V1.0.18 and older, the set_sys_init function in the login.cgi binary allows an attacker to reset the password to the administrative interface of the router.	2021-08-06	5	CVE-2021-36708
qt -- qt	An issue has been fixed in Qt versions 5.14.1 and 5.12.7 where QLibrary attempts to load plugins relative to the working directory, allowing attackers to execute arbitrary code via crafted files.	2021-08-09	6.8	CVE-2020-24741
qt -- qt	An issue has been fixed in Qt versions 5.14.0 where QPluginLoader attempts to load plugins relative to the working directory, allowing attackers to execute arbitrary code via crafted files.	2021-08-09	6.8	CVE-2020-24742
rconfig -- rconfig	The userLogin parameter in ldap/login.php of rConfig 3.9.5 is unsanitized, allowing attackers to perform a LDAP injection and obtain sensitive information via a crafted POST request.	2021-08-09	5	CVE-2020-23148
rconfig -- rconfig	The dbName parameter in ajaxDbInstall.php of rConfig 3.9.5 is unsanitized, allowing attackers to perform a SQL injection and access sensitive database information.	2021-08-09	5	CVE-2020-23149
rconfig -- rconfig	A SQL injection vulnerability in config.inc.php of rConfig 3.9.5 allows attackers to access sensitive database information via a crafted GET request to install/lib/ajaxHandlers/ajaxDbInstall.php.	2021-08-09	5	CVE-2020-23150
roxy-wi -- roxy-wi	Roxy-WI through 5.2.2.0 allows command injection via /app/funct.py and /api/api_funct.py.	2021-08-07	6.5	CVE-2021-38169
roxy-wi -- roxy-wi	Roxy-WI through 5.2.2.0 allows authenticated SQL injection via select_servers.	2021-08-07	6.5	CVE-2021-38168

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ruspiro-singleton_project -- ruspiro-singleton	An issue was discovered in the ruspiro-singleton crate before 0.4.1 for Rust. In Singleton, Send and Sync do not have bounds checks.	2021-08-08	6.8	CVE-2020-36435
sap -- businessobjects_edge	The File Repository Server (FRS) CORBA listener in SAP BussinessObjects Edge 4.0 allows remote attackers to write to arbitrary files via a full pathname, aka SAP Note 2018681.	2021-08-09	5	CVE-2015-2074
sap -- businessobjects_edge	The File RepositoRy Server (FRS) CORBA listener in SAP BussinessObjects Edge 4.0 allows remote attackers to read arbitrary files via a full pathname, aka SAP Note 2018682.	2021-08-09	5	CVE-2015-2073
sap -- j2ee_engine	** UNSUPPORTED WHEN ASSIGNED ** A cross-site scripting (XSS) vulnerability in SAP J2EE Engine/7.01/Portal/EPP allows remote attackers to inject arbitrary web script via the wsdlLib parameter to /ctcprotocol/Protocol. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-08-09	4.3	CVE-2018-17861 BUGTRAQ FULLDISC
sap -- j2ee_engine	** UNSUPPORTED WHEN ASSIGNED ** A cross-site scripting (XSS) vulnerability in SAP J2EE Engine/7.01/Fiori allows remote attackers to inject arbitrary web script via the sys_jdbc parameter to /TestJDBC_Web/test2. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-08-09	4.3	CVE-2018-17862 BUGTRAQ FULLDISC
sap -- j2ee_engine	** UNSUPPORTED WHEN ASSIGNED ** A cross-site scripting (XSS) vulnerability in SAP J2EE Engine 7.01 allows remote attackers to inject arbitrary web script via the wsdlPath parameter to /ctcprotocol/Protocol. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-08-09	4.3	CVE-2018-17865
sapphireims -- sapphireims	In SapphireIMS 4097_1, it is possible to guess the registered/active usernames of the software from the errors it gives out for each type of user on the Login form. For "Incorrect User" - it gives an error "The application failed to identify the user. Please contact administrator for help." For "Correct User and Incorrect Password" - it gives an error "Authentication failed. Please login again."	2021-08-11	5	CVE-2017-16629
signal-simple_project -- signal-simple	An issue was discovered in the signal-simple crate through 2020-11-15 for Rust. There are unconditional implementations of Send and Sync for SyncChannel<T>.	2021-08-08	6.8	CVE-2020-36446
southsoft -- graduate_management_information_system	Southsoft GMIS 5.0 is vulnerable to CSRF attacks. Attackers can access other users' private information such as photos through CSRF. For example: any student's photo information can be accessed through /gmis/(S([1]))/student/grgl/PotoImageShow/?bh=[2]. Among them, the code in [1] is a random string generated according to the user's login related information. It can protect the user's identity, but it can not effectively prevent unauthorized access. The code in [2] is the student number of any student. The attacker can carry out CSRF attack on the system by modifying [2] without modifying [1].	2021-08-06	6.8	CVE-2021-37381
trendnet -- tew-755ap_firmware	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key.	2021-08-10	5	CVE-2021-28845
wagecms_project -- wage-cms	A cross site request forgery (CSRF) in Wage-CMS 1.5.x-dev allows attackers to arbitrarily add users.	2021-08-06	4.3	CVE-2020-21358
yunucms -- yunucms	Cross Site Scripting (XSS) vulnerability exists in YUNUCMS 1.1.9 via the upurl function in Page.php.	2021-08-12	4.3	CVE-2020-18445

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
3.7designs -- project_status	The pspin_duplicate_post_save_as_new_post function of the Project Status WordPress plugin through 1.6 does not sanitise, validate or escape the post GET parameter passed to it before outputting it in an error message when the related post does not exist, leading to a reflected XSS issue	2021-08-23	3.5	CVE-2021-24558
apache -- portable_runtime	An out-of-bounds array read in the apr_time_exp*() functions was fixed in the Apache Portable Runtime 1.6.3 release (CVE-2017-12613). The fix for this issue was not carried forward to the APR 1.7.x branch, and hence version 1.7.0 regressed compared to 1.6.3 and is vulnerable to the same issue.	2021-08-23	3.6	CVE-2021-35940 CONFIRM CONFIRM CONFIRM CONFIRM MLIST MLIST MLIST
arm -- cortex-m33_firmware	Certain Arm products before 2021-08-23 do not properly consider the effect of exceptions on a VLLDM instruction. A Non-secure handler may have read or write access to part of a Secure context. This affects Arm Cortex-M33 r0p0 through r1p0, Arm Cortex-M35P r0, Arm Cortex-M55 r0p0 through r1p0, and Arm China STAR-MC1 (in the STAR SE configuration).	2021-08-23	3.6	CVE-2021-35465 CONFIRM
awplife -- grid_gallery	The Grid Gallery â€“ Photo Image Grid Gallery WordPress plugin before 1.2.5 does not properly sanitize the title field for image galleries when adding them via the admin dashboard, resulting in an authenticated Stored Cross-Site Scripting vulnerability.	2021-08-23	3.5	CVE-2021-24529
bigtreecms -- bigtree_cms	Cross Site Scripting (XSS) vulnerabilty exists in BigTree-CMS 4.4.3 in the tag name field found in the Tags page under the General menu via a crafted website name by doing an authenticated POST HTTP request to admin/tags/create.	2021-08-26	3.5	CVE-2020-18467
erident_custom_login_and_dashboard_project -- erident_custom_login_and_dashboard	The Erident Custom Login and Dashboard WordPress plugin before 3.5.9 did not properly sanitise its settings, allowing high privilege users to use XSS payloads in them (even when the unfileted_html is disabled)	2021-08-23	3.5	CVE-2021-24658 CONFIRM
gitlab -- gitlab	An issue has been discovered in GitLab affecting all versions starting with 13.3. GitLab was vulnerable to a stored XSS by using the design feature in issues.	2021-08-20	3.5	CVE-2021-22238 CONFIRM
gitlab -- gitlab	Under very specific conditions a user could be impersonated using Gitlab shell. This vulnerability affects GitLab CE/EE 13.1 and later through 14.1.2, 14.0.7 and 13.12.9.	2021-08-20	3.5	CVE-2021-22254 CONFIRM
givewp -- givewp	The GiveWP â€“ Donation Plugin and Fundraising Platform WordPress plugin before 2.12.0 did not escape the Donation Level setting of its Donation Forms, allowing high privilege users to use Cross-Site Scripting payloads in them.	2021-08-23	3.5	CVE-2021-24524
harmonicdesign -- hd_quiz	The HD Quiz WordPress plugin before 1.8.4 does not escape some of its Answers before outputting them in attribute when generating the Quiz, which could lead to Stored Cross-Site Scripting issues	2021-08-23	3.5	CVE-2021-24571
hucart -- hucart	Cross Site Scripting (XSS) vulnerabilty exists in Hucart CMS 5.7.4 is via the mes_title field. The first user inserts a malicious script into the header field of the outbox and sends it to other users. When other users open the email, the malicious code will be executed.	2021-08-26	3.5	CVE-2020-18475
kn_fix_your_title_project -- kn_fix_your_title	The KN Fix Your Title WordPress plugin through 1.0.1 was vulnerable to Authenticated Stored XSS in the separator field.	2021-08-23	3.5	CVE-2021-24547

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qdpm -- qdpm	Cross Site Scripting (XSS) vulnerability exists in qdPM 9.1 in the Heading field found in the Login Page page under the General menu via a crafted website name by doing an authenticated POST HTTP request to /qdPM_9.1/index.php/configuration.	2021-08-26	3.5	CVE-2020-18468
rconfig -- rconfig	A stored cross-site scripting (XSS) vulnerability in the /devices.php function inrConfig 3.9.5 has been fixed for version 3.9.6. This vulnerability allowed remote attackers to perform arbitrary Javascript execution through entering a crafted payload into the 'Model' field then saving.	2021-08-20	3.5	CVE-2020-25352
rukovoditel -- rukovoditel	Stored cross-site scripting (XSS) vulnerability in the Name of application field found in the General Configuration page in Rukovoditel 2.4.1 allows remote attackers to inject arbitrary web script or HTML via a crafted website name by doing an authenticated POST HTTP request to rukovoditel_2.4.1/install/index.php.	2021-08-26	3.5	CVE-2020-18470
rukovoditel -- rukovoditel	Stored cross-site scripting (XSS) vulnerability in the Copyright Text field found in the Application page under the Configuration menu in Rukovoditel 2.4.1 allows remote attackers to inject arbitrary web script or HTML via a crafted website name by doing an authenticated POST HTTP request to /rukovoditel_2.4.1/index.php?module=configuration/save&redirect_to=configuration/application.	2021-08-26	3.5	CVE-2020-18469
simple_banner_project -- simple_banner	The Simple Banner WordPress plugin before 2.10.4 does not sanitise and escape one of its settings, allowing high privilege users such as admin to use Cross-Site Scripting payload even when the unfiltered_html capability is disallowed.	2021-08-23	3.5	CVE-2021-24574 CONFIRM
webfactoryltd -- maintenance	The Maintenance WordPress plugin before 4.03 does not sanitise or escape some of its settings, allowing high privilege users such as admin to se Cross-Site Scripting payload in them (even when the unfiltered_html capability is disallowed), which will be triggered in the frontend	2021-08-23	3.5	CVE-2021-24533
wpbrigade -- simple_social_media_share_buttons	The Simple Social Media Share Buttons â€“ Social Sharing for Everyone WordPress plugin before 3.2.3 did not escape the align and like_button_size parameters of its SSB shortcode, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks.	2021-08-23	3.5	CVE-2021-24486
wpcharitable -- charitable	The Charitable â€“ Donation Plugin WordPress plugin before 1.6.51 is affected by an authenticated stored cross-site scripting vulnerability which was found in the add donation feature.	2021-08-23	3.5	CVE-2021-24531
wpfront -- scroll_top	The WPFront Scroll Top WordPress plugin before 2.0.6.07225 does not sanitise or escape its Image ALT setting before outputting it attributes, leading to an Authenticated Stored Cross-Site Scripting issues even when the unfiltered_html capability is disallowed.	2021-08-23	3.5	CVE-2021-24564
miniorange -- saml	The miniorange_saml (aka Miniorange Saml) extension before 1.4.3 for TYPO3 allows XSS.	2021-08-13	3.5	CVE-2021-36785 CONFIRM
yoast -- yoast_seo	The yoast_seo (aka Yoast SEO) extension before 7.2.3 for TYPO3 allows XSS.	2021-08-13	3.5	CVE-2021-36788 CONFIRM
chikitsa -- patient_management_system	index.php/admin/add_user in Chikitsa Patient Management System 2.0.0 allows XSS.	2021-08-06	3.5	CVE-2021-38149
chikitsa -- patient_management_system	index.php/appointment/insert_patient_add_appointment in Chikitsa Patient Management System 2.0.0 allows XSS.	2021-08-06	3.5	CVE-2021-38152

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
chikitsa -- patient_management_system	index.php/appointment/todos in Chikitsa Patient Management System 2.0.0 allows XSS.	2021-08-06	3.5	CVE-2021-38151
damicms -- damicms	Cross Site Scripting (XSS) vulnerability exists in DamiCMS v6.0.6 via the title parameter in the doadd function in LabelAction.class.php.	2021-08-12	3.5	CVE-2020-18451
eyoucms -- eyoucms	A stored cross site scripting (XSS) vulnerability in the web_copyright field of Eyoucms v1.4.1 allows authenticated attackers to execute arbitrary web scripts or HTML.	2021-08-10	3.5	CVE-2020-21929
eyoucms -- eyoucms	A stored cross site scripting (XSS) vulnerability in the web_attr_2 field of Eyoucms v1.4.1 allows authenticated attackers to execute arbitrary web scripts or HTML.	2021-08-10	3.5	CVE-2020-21930
fortinet -- fortianalyzer	Multiple improper neutralization of input during web page generation (CWE-79) in FortiManager and FortiAnalyzer versions 7.0.0, 6.4.5 and below, 6.2.7 and below user interface, may allow a remote authenticated attacker to perform a Stored Cross Site Scripting attack (XSS) by injecting malicious payload in GET parameters.	2021-08-06	3.5	CVE-2021-32597 CONFIRM
get-simple -- getsimplecms	A stored cross site scripting (XSS) vulnerability in /admin/snippets.php of GetSimple CMS 3.4.0a allows attackers to execute arbitrary web scripts or HTML via crafted payload in the Edit Snippets module.	2021-08-06	3.5	CVE-2020-21353
huawei -- harmonyos	A component of the HarmonyOS has a permission bypass vulnerability. Local attackers may exploit this vulnerability to cause the device to hang due to the page error OsVmPageFaultHandler.	2021-08-06	2.1	CVE-2021-22295
jetbrains -- youtrack	In JetBrains YouTrack before 2021.2.17925, stored XSS was possible.	2021-08-06	3.5	CVE-2021-37552
linux -- linux_kernel	btrfs in the Linux kernel before 5.13.4 allows attackers to cause a denial of service (deadlock) via processes that trigger allocation of new system chunks during times when there is a shortage of free space in the system space_info.	2021-08-08	2.1	CVE-2021-38203
linux -- linux_kernel	arch/x86/kvm/mmu/paging_tmpl.h in the Linux kernel before 5.12.11 incorrectly computes the access permissions of a shadow page, leading to a missing guest protection page fault.	2021-08-08	2.1	CVE-2021-38198
linux -- linux_kernel	net/netfilter/nf_conntrack_standalone.c in the Linux kernel before 5.12.2 allows observation of changes in any net namespace because these changes are leaked into all other net namespaces. This is related to the NF_SYSCTL_CT_MAX, NF_SYSCTL_CT_EXPECT_MAX, and NF_SYSCTL_CT_BUCKETS sysctls.	2021-08-08	2.1	CVE-2021-38209
linux -- linux_kernel	The mac80211 subsystem in the Linux kernel before 5.12.13, when a device supporting only 5 GHz is used, allows attackers to cause a denial of service (NULL pointer dereference in the radiotap parser) by injecting a frame with 802.11a rates.	2021-08-08	2.1	CVE-2021-38206
linux -- linux_kernel	drivers/usb/host/max3421-hcd.c in the Linux kernel before 5.13.6 allows physically proximate attackers to cause a denial of service (use-after-free and panic) by removing a MAX-3421 USB device in certain situations.	2021-08-08	2.1	CVE-2021-38204
linux -- linux_kernel	drivers/net/ethernet/xilinx/xilinx_emaclite.c in the Linux kernel before 5.13.3 makes it easier for attackers to defeat an ASLR protection mechanism because it prints a kernel pointer (i.e., the real IOMEM pointer).	2021-08-08	2.1	CVE-2021-38205
linux -- linux_kernel	net/nfc/llcp_sock.c in the Linux kernel before 5.12.10 allows local unprivileged users to cause a denial of service (NULL pointer dereference and BUG) by making a getsockname call after a certain type of failure of a bind call.	2021-08-08	2.1	CVE-2021-38208
linux -- linux_kernel	arch/powerpc/perf/core-book3s.c in the Linux kernel before 5.12.13, on systems with perf_event_paranoid=-1 and no specific PMU driver support registered, allows local users to cause a denial of service (perf_instruction_pointer NULL pointer dereference and OOPS) via a "perf record" command.	2021-08-08	2.1	CVE-2021-38200

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
maccms -- maccms	A cross site scripting (XSS) vulnerability in the background search function of Maccms10 allows attackers to execute arbitrary web scripts or HTML via the 'wd' parameter.	2021-08-11	3.5	CVE-2020-21362
mineweb_project -- minewebcms	Cross Site Scripting (XSS) in MineWebCMS v1.7.0 allows remote attackers to execute arbitrary code by injecting malicious code into the 'Title' field of the component '/admin/news'.	2021-08-06	3.5	CVE-2020-18693
naviwebs -- navigate_cms	Cross Site Scripting (XSS) vulnerability in Naviwebs Navigate Cms 2.9 via the navigate-quickse parameter to 1) backups\backups.php, 2) blocks\blocks.php, 3) brands\brands.php, 4) comments\comments.php, 5) coupons\coupons.php, 6) feeds\feeds.php, 7) functions\functions.php, 8) items\items.php, 9) menus\menus.php, 10) orders\orders.php, 11) payment_methods\payment_methods.php, 12) products\products.php, 13) profiles\profiles.php, 14) shipping_methods\shipping_methods.php, 15) templates\templates.php, 16) users\users.php, 17) webdictionary\webdictionary.php, 18) websites\websites.php, and 19) webusers\webusers.php because the initial_url function is built in these files.	2021-08-06	3.5	CVE-2021-36454
ukcms -- ukcms	Cross Site Scripting (XSS) vulnerability exists in UKCMS v1.1.10 via data in the index function in Single.php	2021-08-12	3.5	CVE-2020-18449
ukcms_project -- ukcms	A stored cross site scripting (XSS) vulnerability in index.php/legend/6.html of UK CMS v1.1.10 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the Comments section.	2021-08-12	3.5	CVE-2020-20977
yunucms -- yunucms	Cross Site Scripting (XSS) vulnerability exists in YUNUCMS 1.1.9 via the param parameter in the insertContent function in ContentModel.php.	2021-08-12	3.5	CVE-2020-18446