SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 15 December 2021

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-38503	The iframe sandbox rules were not correctly applied to XSLT stylesheets, allowing an iframe to bypass restrictions such as executing scripts or navigating the top-level frame. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.	10.0	More Details
CVE-2021-21951	An out-of-bounds write vulnerability exists in the CMD_DEVICE_GET_SERVER_LIST_REQUEST functionality of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h in function read_udp_push_config_file. A specially-crafted network packet can lead to code execution.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44228	Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.	10.0	More Details
CVE-2021-21950	An out-of-bounds write vulnerability exists in the CMD_DEVICE_GET_SERVER_LIST_REQUEST functionality of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h in function recv_server_device_response_msg_process. A specially-crafted network packet can lead to code execution.	10.0	More Details
CVE-2021-43821	Opencast is an Open Source Lecture Capture & Video Management for Education. Opencast before version 9.10 or 10.6 allows references to local file URLs in ingested media packages, allowing attackers to include local files from Opencast's host machines and making them available via the web interface. Before Opencast 9.10 and 10.6, Opencast would open and include local files during ingests. Attackers could exploit this to include most local files the process has read access to, extracting secrets from the host machine. An attacker would need to have the privileges required to add new media to exploit this. But these are often widely given. The issue has been fixed in Opencast 10.6 and 11.0. You can mitigate this issue by narrowing down the read access Opencast has to files on the file system using UNIX permissions or mandatory access control systems like SELinux. This cannot prevent access to files Opencast needs to read though and we highly recommend updating.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43802	Etherpad is a real-time collaborative editor. In versions prior to 1.8.16, an attacker can craft an `*.etherpad` file that, when imported, might allow the attacker to gain admin privileges for the Etherpad instance. This, in turn, can be used to install a malicious Etherpad plugin that can execute arbitrary code (including system commands). To gain privileges, the attacker must be able to trigger deletion of `express-session` state or wait for old `express-session` state to be cleaned up. Core Etherpad does not delete any `express-session` state, so the only known attacks require either a plugin that can delete session state or a custom cleanup process (such as a cron job that deletes old `sessionstorage:*` records). The problem has been fixed in version 1.8.16. If users cannot upgrade to 1.8.16 or install patches manually, several workarounds are available. Users may configure their reverse proxies to reject requests to `/p/*/import`, which will block all imports, not just `*.etherpad` imports; limit all users to read-only access; and/or prevent the reuse of `express_sid` cookie values that refer to deleted express-session state. More detailed information and general mitigation strategies may be found in the GitHub Security Advisory.	9.9	More Details
CVE-2021-21954	A command execution vulnerability exists in the wifi_country_code_update functionality of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h. A specially-crafted set of network packets can lead to arbitrary command execution.	9.9	More Details
CVE-2021-24946	The Modern Events Calendar Lite WordPress plugin before 6.1.5 does not sanitise and escape the time parameter before using it in a SQL statement in the mec_load_single_page AJAX action, available to unauthenticated users, leading to an unauthenticated SQL injection issue	9.8	More Details
CVE-2021-43117	fastadmin v1.2.1 is affected by a file upload vulnerability which allows arbitrary code execution through shell access.	9.8	More Details
CVE-2021-24951	The LearnPress WordPress plugin before 4.1.4 does not sanitise, validate and escape the id parameter before using it in SQL statements when duplicating course/lesson/quiz/question, leading to SQL Injections issues	9.8	More Details
CVE-2021-24863	The WP Block and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection Plugin StopBadBots WordPress plugin before 6.67 does not sanitise and escape the User Agent before using it in a SQL statement to save it, leading to a SQL injection	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22279	A Missing Authentication vulnerability in RobotWare for the OmniCore robot controller allows an attacker to read and modify files on the robot controller if the attacker has access to the Connected Services Gateway Ethernet port.	9.8	More Details
CVE-2021-24857	The ToTop Link WordPress plugin through 1.7.1 passes base64 encoded user input to the unserialize() PHP function, which could lead to PHP Object injection if a plugin installed on the blog has a suitable gadget chain.	9.8	More Details
CVE-2021-44152	An issue was discovered in Reprise RLM 14.2. Because /goform/change_password_process does not verify authentication or authorization, an unauthenticated user can change the password of any existing user. This allows an attacker to change the password of any known user, thereby preventing valid users from accessing the system and granting the attacker full access to that user's account.	9.8	More Details
CVE-2021-44847	A stack-based buffer overflow in handle_request function in DHT.c in toxcore 0.1.9 through 0.1.11 and 0.2.0 through 0.2.12 (caused by an improper length calculation during the handling of received network packets) allows remote attackers to crash the process or potentially execute arbitrary code via a network packet.	9.8	More Details
CVE-2021-44833	The CLI 1.0.0 for Amazon AWS OpenSearch has weak permissions for the configuration file.	9.8	More Details
CVE-2021-44515	Zoho ManageEngine Desktop Central is vulnerable to authentication bypass, leading to remote code execution on the server, as exploited in the wild in December 2021. For Enterprise builds 10.1.2127.17 and earlier, upgrade to 10.1.2127.18. For Enterprise builds 10.1.2128.0 through 10.1.2137.2, upgrade to 10.1.2137.3. For MSP builds 10.1.2127.17 and earlier, upgrade to 10.1.2127.18. For MSP builds 10.1.2128.0 through 10.1.2137.2, upgrade to 10.1.2137.3.	9.8	More Details
CVE-2021-44966	SQL injection bypass authentication vulnerability in PHPGURUKUL Employee Record Management System 1.2 via index.php. An attacker can log in as an admin account of this system and can destroy, change or manipulate all sensitive information on the system.	9.8	More Details
CVE-2021-39065	IBM Spectrum Copy Data Management 2.2.13 and earlier could allow a remote attacker to execute arbitrary commands on the system, caused by improper validation of user-supplied input by the Spectrum Copy Data Management Admin Console login and uploadcertificate function . A remote attacker could inject arbitrary shell commands which would be executed on the affected system. IBM X-Force ID: 214958.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39052	IBM Spectrum Copy Data Management 2.2.13 and earlier could allow a remote attacker to access the Spring Boot console without authorization. IBM X-Force ID: 214523.	9.8	More Details
CVE-2021-20042	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	9.8	More Details
CVE-2021-32024	A remote code execution vulnerability in the BMP image codec of BlackBerry QNX SDP version(s) 6.4 to 7.1 could allow an attacker to potentially execute code in the context of the affected process.	9.8	More Details
CVE-2021-24045	A type confusion vulnerability could be triggered when resolving the "typeof" unary operator in Facebook Hermes prior to v0.10.0. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected.	9.8	More Details
CVE-2021-44524	A vulnerability has been identified in SiPass integrated V2.76 (All versions), SiPass integrated V2.80 (All versions), SiPass integrated V2.85 (All versions), Siveillance Identity V1.5 (All versions), Siveillance Identity V1.6 (All versions < V1.6.284.0). Affected applications insufficiently limit the access to the internal user authentication service. This could allow an unauthenticated remote attacker to trigger several actions on behalf of valid user accounts.	9.8	More Details
CVE-2021-44538	The olm_session_describe function in Matrix libolm before 3.2.7 is vulnerable to a buffer overflow. The Olm session object represents a cryptographic channel between two parties. Therefore, its state is partially controllable by the remote party of the channel. Attackers can construct a crafted sequence of messages to manipulate the state of the receiver's session in such a way that, for some buffer sizes, a buffer overflow happens on a call to olm_session_describe. Furthermore, safe buffer sizes were undocumented. The overflow content is partially controllable by the attacker and limited to ASCII spaces and digits. The known affected products are Element Web And SchildiChat Web.	9.8	More Details
CVE-2021-45014	There is an upload sql injection vulnerability in the background of taocms 3.0.2 in parameter id:action=cms&ctrl=update&id=26	9.8	More Details
CVE-2021-44949	glFusion CMS 1.7.9 is affected by an access control vulnerability via /public_html/users.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42064	If configured to use an Oracle database and if a query is created using the flexible search java api with a parameterized "in" clause, SAP Commerce - versions 1905, 2005, 2105, 2011, allows attacker to execute crafted database queries, exposing backend database. The vulnerability is present if the parameterized "in" clause accepts more than 1000 values.	9.8	More Details
CVE-2021-44231	Internally used text extraction reports allow an attacker to inject code that can be executed by the application. An attacker could thereby control the behavior of the application.	9.8	More Details
CVE-2021-4073	The RegistrationMagic WordPress plugin made it possible for unauthenticated users to log in as any site user, including administrators, if they knew a valid username on the site due to missing identity validation in the social login function social_login_using_email() of the plugin. This affects versions equal to, and less than, 5.0.1.7.	9.8	More Details
CVE-2021-44041	UiPath Assistant 21.4.4 will load and execute attacker controlled data from the file path supplied to the --dev-widget argument of the URI handler for uipath-assistant://. This allows an attacker to execute code on a victim's machine or capture NTLM credentials by supplying a networked or WebDAV file path.	9.8	More Details
CVE-2021-44042	An issue was discovered in UiPath Assistant 21.4.4. User-controlled data supplied to the --process-start argument of the URI handler for uipath-assistant:// is not correctly encoded, resulting in attacker-controlled content being injected into the error message displayed (when the injected content does not match an existing process). A determined attacker could leverage this to execute JavaScript in the context of the Electron application.	9.8	More Details
CVE-2021-40883	A Remote Code Execution (RCE) vulnerability exists in emlog 5.3.1 via content/plugins.	9.8	More Details
CVE-2021-23639	The package md-to-pdf before 5.0.0 are vulnerable to Remote Code Execution (RCE) due to utilizing the library gray-matter to parse front matter content, without disabling the JS engine.	9.8	More Details
CVE-2021-20038	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27983	Remote Code Execution (RCE) vulnerability exists in MaxSite CMS v107.5 via the Documents page.	9.8	More Details
CVE-2021-3817	wbce_cms is vulnerable to Improper Neutralization of Special Elements used in an SQL Command	9.8	More Details
CVE-2021-27860	A vulnerability in the web management interface of FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p92 and 10.2.2r44p1 allows a remote, unauthenticated attacker to upload a file to any location on the filesystem. The FatPipe advisory identifier for this vulnerability is FPSA006.	9.8	More Details
CVE-2021-3815	utils.js is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	9.8	More Details
CVE-2021-37045	There is an UAF vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the device to restart unexpectedly and the kernel-mode code to be executed.	9.8	More Details
CVE-2021-41063	SQL injection vulnerability was discovered in Aanderaa GeoView Webservice prior to version 2.1.3 that could allow an unauthenticated attackers to execute arbitrary commands.	9.8	More Details
CVE-2021-37040	There is a Parameter injection vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause privilege escalation of files after CIFS share mounting.	9.8	More Details
CVE-2020-27416	Mahavitaran android application 7.50 and prior are affected by account takeover due to improper OTP validation, allows remote attackers to control a users account.	9.8	More Details
CVE-2021-31746	Zip Slip vulnerability in Pluck-CMS Pluck 4.7.15 allows an attacker to upload specially crafted zip files, resulting in directory traversal and potentially arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43527	NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS \#7, or PKCS \#12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS. *Note: This vulnerability does NOT impact Mozilla Firefox.* However, email clients and PDF viewers that use NSS for signature verification, such as Thunderbird, LibreOffice, Evolution and Evince are believed to be impacted. This vulnerability affects NSS < 3.73 and NSS < 3.68.1.	9.8	More Details
CVE-2021-44529	A code injection vulnerability in the Ivanti EPM Cloud Services Appliance (CSA) allows an unauthenticated user to execute arbitrary code with limited permissions (nobody).	9.8	More Details
CVE-2021-37049	There is a Heap-based buffer overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may rewrite the memory of adjacent objects.	9.8	More Details
CVE-2021-20146	An unprotected ssh private key exists on the Gryphon devices which could be used to achieve root access to a server affiliated with Gryphon's development and infrastructure. At the time of discovery, the ssh key could be used to login to the development server hosted in Amazon Web Services.	9.8	More Details
CVE-2021-41694	An Incorrect Access Control vulnerability exists in Premiumdatingscript 4.2.7.7 via the password change procedure in requests\user.php.	9.8	More Details
CVE-2021-41695	An SQL Injection vulnerability exists in Premiumdatingscript 4.2.7.7 via the ip parameter in connect.php. .	9.8	More Details
CVE-2021-20045	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	9.8	More Details
CVE-2021-43703	An Incorrect Access Control vulnerability exists in zzcms less than or equal to 2019 via admin.php. After disabling JavaScript, you can directly access the administrator console.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43608	Doctrine DBAL 3.x before 3.1.4 allows SQL Injection. The escaping of offset and length inputs to the generation of a LIMIT clause was not probably cast to an integer, allowing SQL injection to take place if application developers passed unescaped user input to the DBAL QueryBuilder or any other API that ultimately uses the AbstractPlatform::modifyLimitQuery API.	9.8	More Details
CVE-2021-44514	OpUtils in Zoho ManageEngine OpManager 12.5 before 125490 mishandles authentication for a few audit directories.	9.8	More Details
CVE-2021-35978	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc.	9.8	More Details
CVE-2021-37934	Due to insufficient server-side login-attempt limit enforcement, a vulnerability in /account/login in Huntflow Enterprise before 3.10.14 could allow an unauthenticated, remote user to perform multiple login attempts for brute-force password guessing.	9.8	More Details
CVE-2021-37051	There is an Out-of-bounds read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause out-of-bounds memory access.	9.1	More Details
CVE-2021-44557	National Library of the Netherlands multiNER <= c0440948057afc6e3d6b4903a7c05e666b94a3bc is affected by an XML External Entity (XXE) vulnerability in multiNER/ner.py. Since XML parsing resolves external entities, a malicious XML stream could leak internal files and/or cause a DoS.	9.1	More Details
CVE-2021-44556	National Library of the Netherlands digger < 6697d1269d981e35e11f240725b16401b5ce3db5 is affected by a XML External Entity (XXE) vulnerability. Since XML parsing resolves external entities, a malicious XML stream could leak internal files and/or cause a DoS.	9.1	More Details
CVE-2021-38917	IBM PowerVM Hypervisor FW860, FW940, and FW950 could allow an attacker that gains service access to the FSP can read and write arbitrary host system memory through a series of carefully crafted service procedures. IBM X-Force ID: 210018.	9.1	More Details
CVE-2021-45015	taocms 3.0.2 is vulnerable to arbitrary file deletion via taocms\include\Model\file.php from line 60 to line 72.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44935	glFusion CMS v1.7.9 is affected by an arbitrary user impersonation vulnerability in /public_html/comment.php. The attacker can complete the attack remotely without interaction.	9.1	More Details
CVE-2021-44523	A vulnerability has been identified in SiPass integrated V2.76 (All versions), SiPass integrated V2.80 (All versions), SiPass integrated V2.85 (All versions), Siveillance Identity V1.5 (All versions), Siveillance Identity V1.6 (All versions < V1.6.284.0). Affected applications insufficiently limit the access to the internal activity feed database. This could allow an unauthenticated remote attacker to read, modify or delete activity feed entries.	9.1	More Details
CVE-2021-23859	An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter Modified CVSS Scores for CVE-2021-23859	9.1	More Details
CVE-2021-4048	An out-of-bounds read flaw was found in the CLARRV, DLARRV, SLARRV, and ZLARRV functions in lapack through version 3.10.0, as also used in OpenBLAS before version 0.3.18. Specially crafted inputs passed to these functions could cause an application using lapack to crash or possibly disclose portions of its memory.	9.1	More Details
CVE-2021-39063	IBM Spectrum Protect Plus 10.1.0.0 through 10.1.8.x uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information due to a misconfiguration in access control headers. IBM X-Force ID: 214956.	9.1	More Details
CVE-2021-24922	The Pixel Cat WordPress plugin before 2.6.2 does not have CSRF check when saving its settings, and did not sanitise as well as escape some of them, which could allow attacker to make a logged in admin change them and perform Cross-Site Scripting attacks	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45046	It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-22568	When using the dart pub publish command to publish a package to a third-party package server, the request would be authenticated with an oauth2 access_token that is valid for publishing on pub.dev. Using these obtained credentials, an attacker can impersonate the user on pub.dev. We recommend upgrading past https://github.com/dart-lang/sdk/commit/d787e78d21e12ec1ef712d229940b1172aafcdf8 or beyond version 2.15.0	8.8	More Details
CVE-2021-37188	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway.	8.8	More Details
CVE-2021-38510	The executable file warning was not presented when downloading .inetloc files, which, due to a flaw in Mac OS, can run commands on a user's computer.*Note: This issue only affected Mac OS operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.	8.8	More Details
CVE-2021-44233	SAP GRC Access Control - versions V1100_700, V1100_731, V1200_750, does not perform necessary authorization checks for an authenticated user, which could lead to escalation of privileges.	8.8	More Details
CVE-2020-19682	A Cross Site Request Forgery (CSRF) vulnerability exits in ZZZCMS V1.7.1 via the save_user funciton in save.php.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40282	An SQL Injection vulnerability exists in zzcms 8.2, 8.3, 2020, abd 2021 in dl/dl_download.php. when registering ordinary users.	8.8	More Details
CVE-2021-40281	An SQL Injection vulnerability exists in zzcms 8.2, 8.3, 2020, and 2021 in dl/dl_print.php when registering ordinary users.	8.8	More Details
CVE-2021-43534	Mozilla developers and community members reported memory safety bugs present in Firefox 93 and Firefox ESR 91.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.	8.8	More Details
CVE-2021-43535	A use-after-free could have occured when an HTTP2 session object was released on a different thread, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.3, and Firefox ESR < 91.3.	8.8	More Details
CVE-2021-43537	An incorrect type conversion of sizes from 64bit to 32bit integers allowed an attacker to corrupt memory leading to a potentially exploitable crash. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95.	8.8	More Details
CVE-2021-20144	An unauthenticated command injection vulnerability exists in the parameters of operation 49 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.	8.8	More Details
CVE-2021-20143	An unauthenticated command injection vulnerability exists in the parameters of operation 48 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.	8.8	More Details
CVE-2021-20142	An unauthenticated command injection vulnerability exists in the parameters of operation 41 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20141	An unauthenticated command injection vulnerability exists in the parameters of operation 32 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.	8.8	More Details
CVE-2021-20140	An unauthenticated command injection vulnerability exists in the parameters of operation 10 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.	8.8	More Details
CVE-2021-20139	An unauthenticated command injection vulnerability exists in the parameters of operation 3 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.	8.8	More Details
CVE-2021-20138	An unauthenticated command injection vulnerability exists in multiple parameters in the Gryphon Tower router's web interface at /cgi-bin/luci/rc. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the web interface.	8.8	More Details
CVE-2021-43071	A heap-based buffer overflow in Fortinet FortiWeb version 6.4.1 and 6.4.0, version 6.3.15 and below, version 6.2.6 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests to the LogReport API controller.	8.8	More Details
CVE-2021-43539	Failure to correctly record the location of live pointers across wasm instance calls resulted in a GC occurring within the call not tracing those live pointers. This could have led to a use-after-free causing a potentially exploitable crash. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95.	8.8	More Details
CVE-2021-38504	When interacting with an HTML input element's file picker dialog with webkitdirectory set, a use-after-free could have resulted, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.	8.8	More Details
CVE-2021-42760	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiWLM version 8.6.1 and below allows attacker to disclose sensitive information from DB tables via crafted requests.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36719	PineApp - Mail Secure - The attacker must be logged in as a user to the Pineapp system. The attacker exploits the vulnerable nicUpload.php file to upload a malicious file,Thus taking over the server and running remote code.	8.8	More Details
CVE-2021-20044	A post-authentication remote command injection vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	8.8	More Details
CVE-2021-24848	The mediamaticAjaxRenameCategory AJAX action of the Mediamatic WordPress plugin before 2.8.1, available to any authenticated user, does not sanitise the categoryID parameter before using it in a SQL statement, leading to an SQL injection	8.8	More Details
CVE-2021-38182	Due to insufficient input validation of Kyma, authenticated users can pass a Header of their choice and escalate privileges which can completely compromise the cluster.	8.8	More Details
CVE-2021-3376	An issue was discovered in Cuppa CMS Versions Before 31 Jan 2021 allows authenticated attackers to gain escalated privileges via a crafted POST request using the user_group_id_field parameter.	8.8	More Details
CVE-2021-40857	Auerswald COMpact 5500R devices before 8.2B allow Privilege Escalation via the passwd=1 substring.	8.8	More Details
CVE-2021-44726	KNIME Server before 4.13.4 allows XSS via the old WebPortal login page.	8.8	More Details
CVE-2021-41805	HashiCorp Consul Enterprise before 1.8.17, 1.9.x before 1.9.11, and 1.10.x before 1.10.4 has Incorrect Access Control. An ACL token (with the default operator:write permissions) in one namespace can be used for unintended privilege escalation in a different namespace.	8.8	More Details
CVE-2021-20039	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a remote authenticated attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	8.8	More Details
CVE-2021-42758	An improper access control vulnerability [CWE-284] in FortiWLC 8.6.1 and below may allow an authenticated and remote attacker with low privileges to execute any command as an admin user with full access rights via bypassing the GUI restrictions.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20043	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	8.8	More Details
CVE-2021-36194	Multiple stack-based buffer overflows in the API controllers of FortiWeb 6.4.1, 6.4.0, and 6.3.0 through 6.3.15 may allow an authenticated attacker to achieve arbitrary code execution via specially crafted requests.	8.8	More Details
CVE-2021-41017	Multiple heap-based buffer overflow vulnerabilities in some web API controllers of FortiWeb 6.4.1, 6.4.0, and 6.3.0 through 6.3.15 may allow a remote authenticated attacker to execute arbitrary code or commands via specifically crafted HTTP requests.	8.8	More Details
CVE-2021-29678	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a user with DBADM authority to access other databases and read or modify files. IBM X-Force ID: 199914.	8.7	More Details
CVE-2021-43822	Jackalope Doctrine-DBAL is an implementation of the PHP Content Repository API (PHPCR) using a relational database to persist data. In affected versions users can provoke SQL injections if they can specify a node name or query. Upgrade to version 1.7.4 to resolve this issue. If that is not possible, you can escape all places where `$property` is used to filter `sv:name` in the class `Jackalope\Transport\DoctrineDBAL\Query\QOMWalker`: `XPath::escape($property)`. Node names and xpaths can contain `'` or `;` according to the JCR specification. The jackalope component that translates the query object model into doctrine dbal queries does not properly escape the names and paths, so that a accordingly crafted node name can lead to an SQL injection. If queries are never done from user input, or if you validate the user input to not contain `;`, you are not affected.	8.5	More Details
CVE-2021-26340	A malicious hypervisor in conjunction with an unprivileged attacker process inside an SEV/SEV-ES guest VM may fail to flush the Translation Lookaside Buffer (TLB) resulting in unexpected behavior inside the virtual machine (VM).	8.4	More Details
CVE-2021-43067	A exposure of sensitive information to an unauthorized actor in Fortinet FortiAuthenticator version 6.4.0, version 6.3.2 and below, version 6.2.1 and below, version 6.1.2 and below, version 6.0.7 to 6.0.1 allows attacker to duplicate a target LDAP user 2 factors authentication token via crafted HTTP requests.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43818	lxml is a library for processing XML and HTML in the Python language. Prior to version 4.6.5, the HTML Cleaner in lxml.html lets certain crafted script content pass through, as well as script content in SVG files embedded using data URIs. Users that employ the HTML cleaner in a security relevant context should upgrade to lxml 4.6.5 to receive a patch. There are no known workarounds available.	8.2	More Details
CVE-2021-43817	Collabora Online is a collaborative online office suite based on LibreOffice technology. In affected versions a reflected XSS vulnerability was found in Collabora Online. An attacker could inject unescaped HTML into a variable as they created the Collabora Online iframe, and execute scripts inside the context of the Collabora Online iframe. This would give access to a small set of user settings stored in the browser, as well as the session's authentication token which was also passed in at iframe creation time. Users should upgrade to Collabora Online 6.4.16 or higher or Collabora Online 4.2.20 or higher. Collabora Online Development Edition 21.11 is not affected.	8.2	More Details
CVE-2021-39183	Owncast is an open source, self-hosted live video streaming and chat server. In affected versions inline scripts are executed when Javascript is parsed via a paste action. This issue is patched in 0.0.9 by blocking unsafe-inline Content Security Policy and specifying the script-src. The worker-src is required to be set to blob for the video player.	8.2	More Details
CVE-2021-41242	OpenOlat is a web-basedlearning management system. A path traversal vulnerability exists in OpenOlat prior to versions 15.5.12 and 16.0.5. By providing a filename that contains a relative path as a parameter in some REST methods, it is possible to create directory structures and write files anywhere on the target system. The attack could be used to write files anywhere in the web root folder or outside, depending on the configuration of the system and the properly configured permission of the application server user. The attack requires an OpenOlat user account, an enabled REST API and the rights on a business object to call the vulnerable REST calls. The problem is fixed in version 15.5.12 and 16.0.5. There is a workaround available. The vulnerability requires the REST module to be enabled. Disabling the REST module or limiting the REST module via some firewall or web-server access rules to be accessed only be trusted systems will mitigate the risk.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41265	Flask-AppBuilder is a development framework built on top of Flask. Verions prior to 3.3.4 contain an improper authentication vulnerability in the REST API. The issue allows for a malicious actor with a carefully crafted request to successfully authenticate and gain access to existing protected REST API endpoints. This only affects non database authentication types and new REST API endpoints. Users should upgrade to Flask-AppBuilder 3.3.4 to receive a patch.	8.1	More Details
CVE-2021-26109	An integer overflow or wraparound vulnerability in the memory allocator of SSLVPN in FortiOS before 7.0.1 may allow an unauthenticated attacker to corrupt control data on the heap via specifically crafted requests to SSLVPN, resulting in potentially arbitrary code execution.	8.1	More Details
CVE-2021-39057	IBM Spectrum Protect Plus 10.1.0.0 through 10.1.8.x is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 214616.	8.1	More Details
CVE-2021-37074	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to the user root privilege escalation.	8.1	More Details
CVE-2021-36180	Multiple improper neutralization of special elements used in a command vulnerabilities [CWE-77] in FortiWeb management interface 6.4.1 and below, 6.3.15 and below, 6.2.5 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests.	8.1	More Details
CVE-2021-27984	In Pluck-4.7.15 admin background a remote command execution vulnerability exists when uploading files.	8.1	More Details
CVE-2021-23463	The package com.h2database:h2 from 1.4.198 and before 2.0.202 are vulnerable to XML External Entity (XXE) Injection via the org.h2.jdbc.JdbcSQLXML class object, when it receives parsed string data from org.h2.jdbc.JdbcResultSet.getSQLXML() method. If it executes the getSource() method when the parameter is DOMSource.class it will trigger the vulnerability.	8.1	More Details
CVE-2021-36173	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24945	The Like Button Rating ♥ LikeBtn WordPress plugin before 2.6.38 does not have any authorisation and CSRF checks in the likebtn_export_votes AJAX action, which could allow any authenticated user, such as subscriber, to get a list of email and IP addresses of people who liked content from the blog.	8.0	More Details
CVE-2021-43811	Sockeye is an open-source sequence-to-sequence framework for Neural Machine Translation built on PyTorch. Sockeye uses YAML to store model and data configurations on disk. Versions below 2.3.24 use unsafe YAML loading, which can be made to execute arbitrary code embedded in config files. An attacker can add malicious code to the config file of a trained model and attempt to convince users to download and run it. If users run the model, the embedded code will run locally. The issue is fixed in version 2.3.24.	7.8	More Details
CVE-2021-43065	A incorrect permission assignment for critical resource in Fortinet FortiNAC version 9.2.0, version 9.1.3 and below, version 8.8.9 and below allows attacker to gain higher privileges via the access to sensitive system data.	7.8	More Details
CVE-2021-41021	A privilege escalation vulnerability in FortiNAC versions 8.8.8 and below and 9.1.2 and below may allow an admin user to escalate the privileges to root via the sudo command.	7.8	More Details
CVE-2021-44002	A vulnerability has been identified in JT Open (All versions < V11.1.1.0), JT Utilities (All versions < V13.1.1.0), Solid Edge (All versions < V2023). The Jt1001.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15058, ZDI-CAN-19076, ZDI-CAN-19077)	7.8	More Details
CVE-2021-4007	Rapid7 Insight Agent, versions 3.0.1 to 3.1.2.34, suffer from a local privilege escalation due to an uncontrolled DLL search path. Specifically, when Insight Agent versions 3.0.1 to 3.1.2.34 start, the Python interpreter attempts to load python3.dll at "C:\DLLs\python3.dll," which normally is writable by locally authenticated users. Because of this, a malicious local user could use Insight Agent's startup conditions to elevate to SYSTEM privileges. This issue was fixed in Rapid7 Insight Agent 3.1.2.35. This vulnerability is a regression of CVE-2019-5629.	7.8	More Details
CVE-2021-44001	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The DL180pdfl.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14974)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43983	WECON LeviStudioU Versions 2019-09-21 and prior are vulnerable to multiple stack-based buffer overflow instances while parsing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2020-16154	The App::cpanminus package 1.7044 for Perl allows Signature Verification Bypass.	7.8	More Details
CVE-2020-16156	CPAN 2.28 allows Signature Verification Bypass.	7.8	More Details
CVE-2021-42024	A vulnerability has been identified in Simcenter STAR-CCM+ Viewer (All versions < 2021.3.1). The starview+.exe application lacks proper validation of user-supplied data when parsing scene files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-37941	A local privilege escalation issue was found with the APM Java agent, where a user on the system could attach a malicious file to an application running with the APM Java agent. Using this vector, a malicious or compromised user account could use the agent to run commands at a higher level of permissions than they possess. This vulnerability affects users that have set up the agent via the attacher cli 3, the attach API 2, as well as users that have enabled the profiling_inferred_spans_enabled option	7.8	More Details
CVE-2021-44449	A vulnerability has been identified in JT Utilities (All versions < V12.8.1.1), JTTK (All versions < V10.8.1.1). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14830)	7.8	More Details
CVE-2021-43982	Delta Electronics CNCSoft Versions 1.01.30 and prior are vulnerable to a stack-based buffer overflow, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-38950	IBM MQ on HPE NonStop 8.0.4 and 8.1.0 is vulnerable to a privilege escalation attack when SharedBindingsUserId is set to effective. IBM X-ForceID: 211404.	7.8	More Details
CVE-2021-39049	IBM i2 Analyst's Notebook 9.2.0, 9.2.1, and 9.2.2 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and gain lower level privileges. IBM X-Force ID: 214439.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44006	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted TIFF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2021-39050	IBM i2 Analyst's Notebook 9.2.0, 9.2.1, and 9.2.2 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and gain lower level privileges. IBM X-Force ID: 214440.	7.8	More Details
CVE-2021-44005	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted TIFF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2021-44450	A vulnerability has been identified in JT Utilities (All versions < V12.8.1.1), JTTK (All versions < V10.8.1.1). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15055, ZDI-CAN-14915, ZDI-CAN-14865)	7.8	More Details
CVE-2021-44441	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14913)	7.8	More Details
CVE-2021-26110	An improper access control vulnerability [CWE-284] in FortiOS autod daemon 7.0.0, 6.4.6 and below, 6.2.9 and below, 6.0.12 and below and FortiProxy 2.0.1 and below, 1.2.9 and below may allow an authenticated low-privileged attacker to escalate their privileges to super_admin via a specific crafted configuration of fabric automation CLI script and auto-script features.	7.8	More Details
CVE-2021-44438	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14907)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44437	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14906)	7.8	More Details
CVE-2021-44443	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15039)	7.8	More Details
CVE-2021-44439	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14908)	7.8	More Details
CVE-2018-25020	The BPF subsystem in the Linux kernel before 4.17 mishandles situations with a long jump over an instruction sequence where inner instructions require substantial expansions into multiple BPF instructions, leading to an overflow. This affects kernel/bpf/core.c and net/core/filter.c.	7.8	More Details
CVE-2021-44430	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14829)	7.8	More Details
CVE-2021-44442	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14995)	7.8	More Details
CVE-2021-44432	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to stack based buffer overflow while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14845)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44435	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to stack based buffer overflow while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14903)	7.8	More Details
CVE-2021-44433	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains a use after free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14900)	7.8	More Details
CVE-2021-44445	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15054)	7.8	More Details
CVE-2021-44013	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The DL180pdfl.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15103)	7.8	More Details
CVE-2021-44014	A vulnerability has been identified in JT Open (All versions < V11.1.1.0), JT Utilities (All versions < V13.1.1.0), Solid Edge (All versions < V2023). The Jt1001.dll contains a use-after-free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15057, ZDI-CAN-19081)	7.8	More Details
CVE-2021-44446	A vulnerability has been identified in JT Utilities (All versions < V13.0.3.0), JTTK (All versions < V11.0.3.0). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14828, ZDI-CAN-14898)	7.8	More Details
CVE-2021-44447	A vulnerability has been identified in JT Utilities (All versions < V13.0.3.0), JTTK (All versions < V11.0.3.0). JTTK library in affected products contains a use-after-free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14911)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44434	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14902, ZDI-CAN-14866)	7.8	More Details
CVE-2021-44440	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to memory corruption condition while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14912)	7.8	More Details
CVE-2021-20047	SonicWall Global VPN client version 4.10.6 (32-bit and 64-bit) and earlier have a DLL Search Order Hijacking vulnerability. Successful exploitation via a local attacker could result in remote code execution in the target system.	7.8	More Details
CVE-2021-25517	An improper input validation vulnerability in LDFW prior to SMR Dec-2021 Release 1 allows attackers to perform arbitrary code execution.	7.7	More Details
CVE-2021-43814	Rizin is a UNIX-like reverse engineering framework and command-line toolset. In versions up to and including 0.3.1 there is a heap-based out of bounds write in parse_die() when reversing an AMD64 ELF binary with DWARF debug info. When a malicious AMD64 ELF binary is opened by a victim user, Rizin may crash or execute unintended actions. No workaround are known and users are advised to upgrade.	7.7	More Details
CVE-2021-44232	SAF-T Framework Transaction SAFTN_G allows an attacker to exploit insufficient validation of path information provided by normal user, leading to full server directory access. The attacker can see the whole filesystem structure but cannot overwrite, delete, or corrupt arbitrary files on the server.	7.7	More Details
CVE-2021-20373	IBM Db2 9.7, 10.1, 10.5, 11.1, and 11.5 may be vulnerable to an Information Disclosure when using the LOAD utility as under certain circumstances the LOAD utility does not enforce directory restrictions. IBM X-Force ID: 199521.	7.5	More Details
CVE-2021-41450	An HTTP request smuggling attack in TP-Link AX10v1 before v1_211117 allows a remote unauthenticated attacker to DoS the web application via sending a specific HTTP packet.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38951	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available CPU resources. IBM X-Force ID: 211405.	7.5	More Details
CVE-2021-26108	A use of hard-coded cryptographic key vulnerability in the SSLVPN of FortiOS before 7.0.1 may allow an attacker to retrieve the key by reverse engineering.	7.5	More Details
CVE-2021-39002	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	7.5	More Details
CVE-2021-43801	Mercurius is a GraphQL adapter for Fastify. Any users from Mercurius@8.10.0 to 8.11.1 are subjected to a denial of service attack by sending a malformed JSON to `/graphql` unless they are using a custom error handler. The vulnerability has been fixed in https://github.com/mercurius-js/mercurius/pull/678 and shipped as v8.11.2. As a workaround users may use a custom error handler.	7.5	More Details
CVE-2021-21955	An authentication bypass vulnerability exists in the get_aes_key_info_by_packetid() function of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h. Generic network sniffing can lead to password recovery. An attacker can sniff network traffic to trigger this vulnerability.	7.5	More Details
CVE-2021-41014	A uncontrolled resource consumption in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows an unauthenticated attacker to make the httpsd daemon unresponsive via huge HTTP packets	7.5	More Details
CVE-2021-20145	Gryphon Tower routers contain an unprotected openvpn configuration file which can grant attackers access to the Gryphon homebound VPN network which exposes the LAN interfaces of other users' devices connected to the same service. An attacker could leverage this to make configuration changes to, or otherwise attack victims' devices as though they were on an adjacent network.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43828	PatrOwl is a free and open-source solution for orchestrating Security Operations. In versions prior to 1.77 an improper privilege management (IDOR) has been found in PatrowlManager. All imports findings file is placed under /media/imports/<owner_id>/<tmp_file> In that, owner_id is predictable and tmp_file is in format of import_<ownder_id>_<time_created>, for example: import_1_1639213059582.json This filename is predictable and allows anyone without logging in to download all finding import files This vulnerability is capable of allowing unlogged in users to download all finding imports file. Users are advised to update to 1.7.7 as soon as possible. There are no known workarounds.	7.5	More Details
CVE-2021-4104	JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.	7.5	More Details
CVE-2021-41024	A relative path traversal [CWE-23] vulnerabiltiy in FortiOS versions 7.0.0 and 7.0.1 and FortiProxy verison 7.0.0 may allow an unauthenticated, unauthorized attacker to inject path traversal character sequences to disclose sensitive information of the server via the GET request of the login page.	7.5	More Details
CVE-2021-39064	IBM Spectrum Copy Data Management 2.2.13 and earlier has weak authentication and password rules and incorrectly handles default credentials for the Spectrum Copy Data Management Admin console. IBM X-Force ID: 214957.	7.5	More Details
CVE-2021-43803	Next.js is a React framework. In versions of Next.js prior to 12.0.5 or 11.1.3, invalid or malformed URLs could lead to a server crash. In order to be affected by this issue, the deployment must use Next.js versions above 11.1.0 and below 12.0.5, Node.js above 15.0.0, and next start or a custom server. Deployments on Vercel are not affected, along with similar environments where invalid requests are filtered before reaching Next.js. Versions 12.0.5 and 11.1.3 contain patches for this issue.	7.5	More Details
CVE-2021-44965	Directory traversal vulnerability in /admin/includes/* directory for PHPGURUKUL Employee Record Management System 1.2 The attacker can retrieve and download sensitive information from the vulnerable server.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39312	The True Ranker plugin <= 2.2.2 for WordPress allows arbitrary files, including sensitive configuration files such as wp-config.php, to be accessed via the src parameter found in the ~/admin/vendor/datatables/examples/resources/examples.php file.	7.5	More Details
CVE-2021-41066	An issue was discovered in Listary through 6. When Listary is configured as admin, Listary will not ask for permissions again if a user tries to access files on the system from Listary itself (it will bypass UAC protection; there is no privilege validation of the current user that runs via Listary).	7.5	More Details
CVE-2021-20865	Advanced Custom Fields versions prior to 5.11 and Advanced Custom Fields Pro versions prior to 5.11 contain a missing authorization vulnerability in browsing database which may allow a user to browse unauthorized data via unspecified vectors.	7.5	More Details
CVE-2021-44151	An issue was discovered in Reprise RLM 14.2. As the session cookies are small, an attacker can hijack any existing sessions by bruteforcing the 4 hex-character session cookie on the Windows version (the Linux version appears to have 8 characters). An attacker can obtain the static part of the cookie (cookie name) by first making a request to any page on the application (e.g., /goforms/menu) and saving the name of the cookie sent with the response. The attacker can then use the name of the cookie and try to request that same page, setting a random value for the cookie. If any user has an active session, the page should return with the authorized content, when a valid cookie value is hit.	7.5	More Details
CVE-2021-41311	Affected versions of Atlassian Jira Server and Data Center allow attackers with access to an administrator account that has had its access revoked to modify projects' Users & Roles settings, via a Broken Authentication vulnerability in the /plugins/servlet/project-config/PROJECT/roles endpoint. The affected versions are before version 8.19.1.	7.5	More Details
CVE-2021-44725	KNIME Server before 4.13.4 allows directory traversal in a request for a client profile.	7.5	More Details
CVE-2021-40856	Auerswald COMfortel 1400 IP and 2600 IP before 2.8G devices allow Authentication Bypass via the /about/../ substring.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-25021	The TCP Server module in toxcore before 0.2.8 doesn't free the TCP priority queue under certain conditions, which allows a remote attacker to exhaust the system's memory, causing a denial of service (DoS).	7.5	More Details
CVE-2021-41067	An issue was discovered in Listary through 6. Improper implementation of the update process leads to the download of software updates with a /check-update HTTP-based connection. This can be exploited with MITM techniques. Together with the lack of package validation, it can lead to manipulation of update packages that can cause an installation of malicious content.	7.5	More Details
CVE-2021-20040	A relative path traversal vulnerability in the SMA100 upload funtion allows a remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	7.5	More Details
CVE-2021-20041	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100 /fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	7.5	More Details
CVE-2021-40008	There is a memory leak vulnerability in CloudEngine 12800 V200R019C00SPC800, CloudEngine 5800 V200R019C00SPC800, CloudEngine 6800 V200R019C00SPC800 and CloudEngine 7800 V200R019C00SPC800. The software does not sufficiently track and release allocated memory while parse a series of crafted binary messages, which could consume remaining memory. Successful exploit could cause memory exhaust.	7.5	More Details
CVE-2021-44522	A vulnerability has been identified in SiPass integrated V2.76 (All versions), SiPass integrated V2.80 (All versions), SiPass integrated V2.85 (All versions), Siveillance Identity V1.5 (All versions), Siveillance Identity V1.6 (All versions < V1.6.284.0). Affected applications insufficiently limit the access to the internal message broker system. This could allow an unauthenticated remote attacker to subscribe to arbitrary message queues.	7.5	More Details
CVE-2021-31745	Session Fixation vulnerability in login.php in Pluck-CMS Pluck 4.7.15 allows an attacker to sustain unauthorized access to the platform. Because Pluck does not invalidate prior sessions after a password change, access can be sustained even after an administrator performs regular remediation attempts such as resetting their password.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37935	An information disclosure vulnerability in the login page of Huntflow Enterprise before 3.10.4 could allow an unauthenticated, remote user to get information about the domain name of the configured LDAP server. An attacker could exploit this vulnerability by requesting the login page and searching for the "isLdap" JavaScript parameter in the HTML source code.	7.5	More Details
CVE-2021-38947	IBM Spectrum Copy Data Management 2.2.13 and earlier uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 211242.	7.5	More Details
CVE-2021-39053	IBM Spectrum Copy Data Management 2.2.13 and earlier could allow a remote attacker to obtain sensitive information, caused by the improper handling of requests for Spectrum Copy Data Management Admin Console. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 214524.	7.5	More Details
CVE-2021-39058	IBM Spectrum Copy Data Management 2.2.13 and earlier uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 214617.	7.5	More Details
CVE-2021-37189	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session.	7.5	More Details
CVE-2021-41272	Besu is an Ethereum client written in Java. Starting in version 21.10.0, changes in the implementation of the SHL, SHR, and SAR operations resulted in the introduction of a signed type coercion error in values that represent negative values for 32 bit signed integers. Smart contracts that ask for shifts between approximately 2 billion and 4 billion bits (nonsensical but valid values for the operation) will fail to execute and hence fail to validate. In networks where vulnerable versions are mining with other clients or non-vulnerable versions this will result in a fork and the relevant transactions will not be included in the fork. In networks where vulnerable versions are not mining (such as Rinkeby) no fork will result and the validator nodes will stop accepting blocks. In networks where only vulnerable versions are mining the relevant transaction will not be included in any blocks. When the network adds a non-vulnerable version the network will act as in the first case. Besu 21.10.2 contains a patch for this issue. Besu 21.7.4 is not vulnerable and clients can roll back to that version. There is a workaround available: Once a transaction with the relevant shift operations is included in the canonical chain, the only remediation is to make sure all nodes are on non-vulnerable versions.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37052	There is an Exception log vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause address information leakage.	7.5	More Details
CVE-2021-37097	There is a Code Injection vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to system restart.	7.5	More Details
CVE-2021-43807	Opencast is an Open Source Lecture Capture & Video Management for Education. Opencast versions prior to 9.10 allow HTTP method spoofing, allowing to change the assumed HTTP method via URL parameter. This allows attackers to turn HTTP GET requests into PUT requests or an HTTP form to send DELETE requests. This bypasses restrictions otherwise put on these types of requests and aids in cross-site request forgery (CSRF) attacks, which would otherwise not be possible. The vulnerability allows attackers to craft links or forms which may change the server state. This issue is fixed in Opencast 9.10 and 10.0. You can mitigate the problem by setting the `SameSite=Strict` attribute for your cookies. If this is a viable option for you depends on your integrations. We strongly recommend updating in any case.	7.5	More Details
CVE-2021-37050	There is a Missing sensitive data encryption vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-37044	There is a Permission control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability.	7.5	More Details
CVE-2021-37053	There is a Service logic vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause WLAN DoS.	7.5	More Details
CVE-2021-37054	There is an Identity spoofing and authentication bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-37037	There is an Invalid address access vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the device to restart.	7.5	More Details
CVE-2021-43399	The Yubico YubiHSM YubiHSM2 library 2021.08, included in the yubihsm-shell project, does not properly validate the length of some operations including SSH signing requests, and some data operations received from a YubiHSM 2 device.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4044	Internally libssl in OpenSSL calls X509_verify_cert() on the client side to verify a certificate supplied by a server. That function may return a negative return value to indicate an internal error (for example out of memory). Such a negative return value is mishandled by OpenSSL and will cause an IO function (such as SSL_connect() or SSL_do_handshake()) to not indicate success and a subsequent call to SSL_get_error() to return the value SSL_ERROR_WANT_RETRY_VERIFY. This return value is only supposed to be returned by OpenSSL if the application has previously called SSL_CTX_set_cert_verify_callback(). Since most applications do not do this the SSL_ERROR_WANT_RETRY_VERIFY return value from SSL_get_error() will be totally unexpected and applications may not behave correctly as a result. The exact behaviour will depend on the application but it could result in crashes, infinite loops or other similar incorrect responses. This issue is made more serious in combination with a separate bug in OpenSSL 3.0 that will cause X509_verify_cert() to indicate an internal error when processing a certificate chain. This will occur where a certificate does not include the Subject Alternative Name extension but where a Certificate Authority has enforced name constraints. This issue can occur even with valid chains. By combining the two issues an attacker could induce incorrect, application dependent behaviour. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).	7.5	More Details
CVE-2021-37075	There is a Credentials Management Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to confidentiality affected.	7.5	More Details
CVE-2021-37092	There is a Incomplete Cleanup vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to availability affected.	7.5	More Details
CVE-2021-43388	Unisys Cargo Mobile Application before 1.2.29 uses cleartext to store sensitive information, which might be revealed in a backup. The issue is addressed by ensuring that the allowBackup flag (in the manifest) is False.	7.5	More Details
CVE-2021-37069	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to availability affected.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44549	Apache Sling Commons Messaging Mail provides a simple layer on top of JavaMail/Jakarta Mail for OSGi to send mails via SMTPS. To reduce the risk of "man in the middle" attacks additional server identity checks must be performed when accessing mail servers. For compatibility reasons these additional checks are disabled by default in JavaMail/Jakarta Mail. The SimpleMailService in Apache Sling Commons Messaging Mail 1.0 lacks an option to enable these checks for the shared mail session. A user could enable these checks nevertheless by accessing the session via the message created by SimpleMessageBuilder and setting the property mail.smtps.ssl.checkserveridentity to true. Apache Sling Commons Messaging Mail 2.0 adds support for enabling server identity checks and these checks are enabled by default. - https://javaee.github.io/javamail/docs/SSLNOTES.txt - https://javaee.github.io/javamail/docs/api/com/sun/mail/smtp/package-summary.html - https://github.com/eclipse-ee4j/mail/issues/429	7.4	More Details
CVE-2021-43829	PatrOwl is a free and open-source solution for orchestrating Security Operations. In versions prior to 1.7.7 PatrowlManager unrestrictly handle upload files in the findings import feature. This vulnerability is capable of uploading dangerous type of file to server leading to XSS attacks and potentially other forms of code injection. Users are advised to update to 1.7.7 as soon as possible. There are no known workarounds for this issue.	7.4	More Details
CVE-2021-43830	OpenProject is a web-based project management software. OpenProject versions >= 12.0.0 are vulnerable to a SQL injection in the budgets module. For authenticated users with the "Edit budgets" permission, the request to reassign work packages to another budget unsufficiently sanitizes user input in the `reassign_to_id` parameter. The vulnerability has been fixed in version 12.0.4. Versions prior to 12.0.0 are not affected. If you're upgrading from an older version, ensure you are upgrading to at least version 12.0.4. If you are unable to upgrade in a timely fashion, the following patch can be applied: https://github.com/opf/openproject/pull/9983.patch	7.4	More Details
CVE-2021-42027	A vulnerability has been identified in SINUMERIK Edge (All versions < V3.2). The affected software does not properly validate the server certificate when initiating a TLS connection. This could allow an attacker to spoof a trusted entity by interfering in the communication path between the client and the intended server.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43820	Seafile is an open source cloud storage system. A sync token is used in Seafile file syncing protocol to authorize access to library data. To improve performance, the token is cached in memory in seaf-server. Upon receiving a token from sync client or SeaDrive client, the server checks whether the token exist in the cache. However, if the token exists in cache, the server doesn't check whether it's associated with the specific library in the URL. This vulnerability makes it possible to use any valid sync token to access data from any **known** library. Note that the attacker has to first find out the ID of a library which it has no access to. The library ID is a random UUID, which is not possible to be guessed. There are no workarounds for this issue.	7.4	More Details
CVE-2021-41065	An issue was discovered in Listary through 6. An attacker can create a \\.\pipe\Listary.listaryService named pipe and wait for a privileged user to open a session on the Listary installed host. Listary will automatically access the named pipe and the attacker will be able to duplicate the victim's token to impersonate him. This exploit is valid in certain Windows versions (Microsoft has patched the issue in later Windows 10 builds).	7.3	More Details
CVE-2021-21957	A privilege escalation vulnerability exists in the Remote Server functionality of Dream Report ODS Remote Connector 20.2.16900.0. A specially-crafted command injection can lead to elevated capabilities. An attacker can provide a malicious file to trigger this vulnerability.	7.3	More Details
CVE-2021-41027	A stack-based buffer overflow in Fortinet FortiWeb version 6.4.1 and 6.4.0, allows an authenticated attacker to execute unauthorized code or commands via crafted certificates loaded into the device.	7.3	More Details
CVE-2021-41025	Multiple vulnerabilities in the authentication mechanism of confd in FortiWeb versions 6.4.1, 6.4.0, 6.3.0 through 6.3.15, 6.2.0 through 6.2.6, 6.1.0 through 6.1.2, 6.0.0 thorugh 6.0.7, including an instance of concurrent execution using shared resource with improper synchronization and one of authentication bypass by capture-replay, may allow a remote unauthenticated attacker to circumvent the authentication process and authenticate as a legitimate cluster peer.	7.3	More Details
CVE-2021-44420	In Django 2.2 before 2.2.25, 3.1 before 3.1.14, and 3.2 before 3.2.10, HTTP requests for URLs with trailing newlines could bypass upstream access control based on URL paths.	7.3	More Details
CVE-2021-24970	The All-in-One Video Gallery WordPress plugin before 2.5.0 does not sanitise and validate the tab parameter before using it in a require statement in the admin dashboard, leading to a Local File Inclusion issue	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23862	A crafted configuration packet sent by an authenticated administrative user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000).	7.2	More Details
CVE-2021-41547	A vulnerability has been identified in Teamcenter Active Workspace V4.3 (All versions < V4.3.11), Teamcenter Active Workspace V5.0 (All versions < V5.0.10), Teamcenter Active Workspace V5.1 (All versions < V5.1.6), Teamcenter Active Workspace V5.2 (All versions < V5.2.3). The application contains an unsafe unzipping pattern that could lead to a zip path traversal attack. This could allow and attacker to execute a remote shell with admin rights.	7.2	More Details
CVE-2021-40280	An SQL Injection vulnerablitly exits in zzcms 8.2, 8.3, 2020, and 2021 via the id parameter in admin/dl_sendmail.php.	7.2	More Details
CVE-2021-40279	An SQL Injection vulnerability exists in zzcms 8.2, 8.3, 2020, and 2021 via the id parameter in admin/bad.php.	7.2	More Details
CVE-2021-40861	A SQL Injection in the custom filter query component in Genesys intelligent Workload Distribution (IWD) 9.0.017.07 allows an attacker to execute arbitrary SQL queries via the value attribute, with which all data in the database can be extracted and OS command execution is possible depending on the permissions and/or database engine.	7.2	More Details
CVE-2021-40860	A SQL Injection in the custom filter query component in Genesys intelligent Workload Distribution (IWD) before 9.0.013.11 allows an attacker to execute arbitrary SQL queries via the ql_expression parameter, with which all data in the database can be extracted and OS command execution is possible depending on the permissions and/or database engine.	7.2	More Details
CVE-2021-29214	A security vulnerability has been identified in HPE StoreServ Management Console (SSMC). An authenticated SSMC administrator could exploit the vulnerability to inject code and elevate their privilege in SSMC. The scope of this vulnerability is limited to SSMC. Note: The arrays being managed are not impacted by this vulnerability. This vulnerability impacts SSMC versions 3.4 GA to 3.8.1.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44153	An issue was discovered in Reprise RLM 14.2. When editing the license file, it is possible for an admin user to enable an option to run arbitrary executables, as demonstrated by an ISV demo "C:\Windows\System32\calc.exe" entry. An attacker can exploit this to run a malicious binary on startup, or when triggering the Reread/Restart Servers function on the webserver. (Exploitation does not require CVE-2018-15573, because the license file is meant to be changed in the application.)	7.2	More Details
CVE-2021-44154	An issue was discovered in Reprise RLM 14.2. By using an admin account, an attacker can write a payload to /goform/edit_opt, which will then be triggered when running the diagnostics (via /goform/diagnostics_doit), resulting in a buffer overflow.	7.2	More Details
CVE-2021-24747	The SEO Booster WordPress plugin before 3.8 allows for authenticated SQL injection via the "fn_my_ajaxified_dataloader_ajax" AJAX request as the $_REQUEST['order'][0]['dir'] parameter is not properly escaped leading to blind and error-based SQL injections.	7.2	More Details
CVE-2021-44165	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.41), POWER METER SICAM Q100 (All versions < V2.41), POWER METER SICAM Q100 (All versions < V2.41), POWER METER SICAM Q100 (All versions < V2.41). The affected firmware contains a buffer overflow vulnerability in the web application that could allow a remote attacker with engineer or admin priviliges to potentially perform remote code execution.	7.2	More Details
CVE-2021-24861	The Quotes Collection WordPress plugin through 2.5.2 does not validate and escape the bulkcheck parameter before using it in a SQL statement, leading to a SQL injection	7.2	More Details
CVE-2021-39944	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.0 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. A permissions validation flaw allowed group members with a developer role to elevate their privilege to a maintainer on projects they import	7.1	More Details
CVE-2021-43978	Allegro WIndows 3.3.4152.0, embeds software administrator database credentials into its binary files, which allows users to access and modify data using the same credentials.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43051	The Spotfire Server component of TIBCO Software Inc.'s TIBCO Spotfire Server, TIBCO Spotfire Server, and TIBCO Spotfire Server contains a difficult to exploit vulnerability that allows malicious custom API clients with network access to execute internal API operations outside of the scope of those granted to it. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Server: versions 10.10.6 and below, TIBCO Spotfire Server: versions 11.0.0, 11.1.0, 11.2.0, 11.3.0, 11.4.0, and 11.4.1, and TIBCO Spotfire Server: versions 11.5.0 and 11.6.0.	7.1	More Details
CVE-2021-41449	A path traversal attack in web interfaces of Netgear RAX35, RAX38, and RAX40 routers before v1.0.4.102, allows a remote unauthenticated attacker to gain access to sensitive restricted information, such as forbidden files of the web application, via sending a specially crafted HTTP packet.	7.1	More Details
CVE-2021-42110	An issue was discovered in Allegro Windows (formerly Popsy Windows) before 3.3.4156.1. A standard user can escalate privileges to SYSTEM if the FTP module is installed, because of DLL hijacking.	7.1	More Details
CVE-2021-42835	An issue was discovered in Plex Media Server through 1.24.4.5081-e362dc1ee. An attacker (with a foothold in a endpoint via a low-privileged user account) can access the exposed RPC service of the update service component. This RPC functionality allows the attacker to interact with the RPC functionality and execute code from a path of his choice (local, or remote via SMB) because of a TOCTOU race condition. This code execution is in the context of the Plex update service (which runs as SYSTEM).	7.0	More Details
CVE-2021-39935	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.5 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. Unauthorized external users could perform Server Side Requests via the CI Lint API	6.8	More Details
CVE-2021-36189	A missing encryption of sensitive data in Fortinet FortiClientEMS version 7.0.1 and below, version 6.4.4 and below allows attacker to information disclosure via inspecting browser decrypted data	6.8	More Details
CVE-2021-42757	A buffer overflow [CWE-121] in the TFTP client library of FortiOS before 6.4.7 and FortiOS 7.0.0 through 7.0.2, may allow an authenticated local attacker to achieve arbitrary code execution via specially crafted command line arguments.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12890	Improper handling of pointers in the System Management Mode (SMM) handling code may allow for a privileged attacker with physical or administrative access to potentially manipulate the AMD Generic Encapsulated Software Architecture (AGESA) to execute arbitrary code undetected by the operating system.	6.7	More Details
CVE-2021-44235	Two methods of a utility class in SAP NetWeaver AS ABAP - versions 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, allow an attacker with high privileges and has direct access to SAP System, to inject code when executing with a certain transaction class builder. This could allow execution of arbitrary commands on the operating system, that could highly impact the Confidentiality, Integrity and Availability of the system.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43809	`Bundler` is a package for managing application dependencies in Ruby. In `bundler` versions before 2.2.33, when working with untrusted and apparently harmless `Gemfile`'s, it is not expected that they lead to execution of external code, unless that's explicit in the ruby code inside the `Gemfile` itself. However, if the `Gemfile` includes `gem` entries that use the `git` option with invalid, but seemingly harmless, values with a leading dash, this can be false. To handle dependencies that come from a Git repository instead of a registry, Bundler uses various commands, such as `git clone`. These commands are being constructed using user input (e.g. the repository URL). When building the commands, Bundler versions before 2.2.33 correctly avoid Command Injection vulnerabilities by passing an array of arguments instead of a command string. However, there is the possibility that a user input starts with a dash (`-`) and is therefore treated as an optional argument instead of a positional one. This can lead to Code Execution because some of the commands have options that can be leveraged to run arbitrary executables. Since this value comes from the `Gemfile` file, it can contain any character, including a leading dash. To exploit this vulnerability, an attacker has to craft a directory containing a `Gemfile` file that declares a dependency that is located in a Git repository. This dependency has to have a Git URL in the form of `-u./payload`. This URL will be used to construct a Git clone command but will be interpreted as the upload-pack argument. Then this directory needs to be shared with the victim, who then needs to run a command that evaluates the Gemfile, such as `bundle lock`, inside. This vulnerability can lead to Arbitrary Code Execution, which could potentially lead to the takeover of the system. However, the exploitability is very low, because it requires a lot of user interaction. Bundler 2.2.33 has patched this problem by inserting `--` as an argument before any positional arguments to those Git commands that were affected by this issue. Regardless of whether users can upgrade or not, they should review any untrustred `Gemfile`'s before running any `bundler` commands that may read them, since they can contain arbitrary ruby code.	6.7	More Details
CVE-2021-42759	A violation of secure design principles in Fortinet Meru AP version 8.6.1 and below, version 8.5.5 and below allows attacker to execute unauthorized code or commands via crafted cli commands.	6.7	More Details
CVE-2021-24845	The Improved Include Page WordPress plugin through 1.2 allows passing shortcode attributes with post_type & post_status which can be used to retrieve arbitrary content. This way, users with a role as low as Contributor can gain access to content they are not supposed to.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20867	Advanced Custom Fields versions prior to 5.11 and Advanced Custom Fields Pro versions prior to 5.11 contain a missing authorization vulnerability in moving the field group which may allow a user to move the unauthorized field group via unspecified vectors.	6.5	More Details
CVE-2021-38931	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1, and 11.5 is vulnerable to an information disclosure as a result of a connected user having indirect read access to a table where they are not authorized to select from. IBM X-Force ID: 210418.	6.5	More Details
CVE-2021-43540	WebExtensions with the correct permissions were able to create and install ServiceWorkers for third-party websites that would not have been uninstalled with the extension. This vulnerability affects Firefox < 95.	6.5	More Details
CVE-2021-43541	When invoking protocol handlers for external protocols, a supplied parameter URL containing spaces was not properly escaped. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95.	6.5	More Details
CVE-2021-43542	Using XMLHttpRequest, an attacker could have identified installed applications by probing error messages for loading external protocols. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95.	6.5	More Details
CVE-2021-42022	A vulnerability has been identified in SIMATIC eaSie PCS 7 Skill Package (All versions < V21.00 SP3). When downloading files, the affected systems do not properly neutralize special elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read unexpected critical files. The affected file download function is disabled by default.	6.5	More Details
CVE-2021-20866	Advanced Custom Fields versions prior to 5.11 and Advanced Custom Fields Pro versions prior to 5.11 contain a missing authorization vulnerability in obtaining the user list which may allow a user to obtain the unauthorized information via unspecified vectors.	6.5	More Details
CVE-2021-39939	An uncontrolled resource consumption vulnerability in GitLab Runner affecting all versions starting from 13.7 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an attacker triggering a job with a specially crafted docker image to exhaust resources on runner manager	6.5	More Details
CVE-2021-24795	The Filter Portfolio Gallery WordPress plugin through 1.5 is lacking Cross-Site Request Forgery (CSRF) check when deleting a Gallery, which could allow attackers to make a logged in admin delete arbitrary Gallery.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24872	The Get Custom Field Values WordPress plugin before 4.0 allows users with a role as low as Contributor to access other posts metadata without validating the permissions. Eg. contributors can access admin posts metadata.	6.5	More Details
CVE-2021-41696	An authentication bypass (account takeover) vulnerability exists in Premiumdatingscript 4.2.7.7 due to a weak password reset mechanism in requests\user.php.	6.5	More Details
CVE-2021-43545	Using the Location API in a loop could have caused severe application hangs and crashes. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95.	6.5	More Details
CVE-2021-24784	The WP Admin Logo Changer WordPress plugin through 1.0 does not have CSRF check when saving its settings, which could allow attackers to make a logged in admin update them via a CSRF attack.	6.5	More Details
CVE-2021-43823	Sourcegraph is a code search and navigation engine. Sourcegraph prior to version 3.33.2 is vulnerable to a side-channel attack where strings in private source code could be guessed by an authenticated but unauthorized actor. This issue affects the Saved Searches and Code Monitoring features. A successful attack would require an authenticated bad actor to create many Saved Searches or Code Monitors to receive confirmation that a specific string exists. This could allow an attacker to guess formatted tokens in source code, such as API keys. This issue was patched in version 3.33.2 and any future versions of Sourcegraph. We strongly encourage upgrading to secure versions. If you are unable to, you may disable Saved Searches and Code Monitors.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41090	Grafana Agent is a telemetry collector for sending metrics, logs, and trace data to the opinionated Grafana observability stack. Prior to versions 0.20.1 and 0.21.2, inline secrets defined within a metrics instance config are exposed in plaintext over two endpoints: metrics instance configs defined in the base YAML file are exposed at `/-/config` and metrics instance configs defined for the scraping service are exposed at `/agent/api/v1/configs/:key`. Inline secrets will be exposed to anyone being able to reach these endpoints. If HTTPS with client authentication is not configured, these endpoints are accessible to unauthenticated users. Secrets found in these sections are used for delivering metrics to a Prometheus Remote Write system, authenticating against a system for discovering Prometheus targets, and authenticating against a system for collecting metrics. This does not apply for non-inlined secrets, such as `*_file` based secrets. This issue is patched in Grafana Agent versions 0.20.1 and 0.21.2. A few workarounds are available. Users who cannot upgrade should use non-inline secrets where possible. Users may also desire to restrict API access to Grafana Agent with some combination of restricting the network interfaces Grafana Agent listens on through `http_listen_address` in the `server` block, configuring Grafana Agent to use HTTPS with client authentication, and/or using firewall rules to restrict external access to Grafana Agent's API.	6.5	More Details
CVE-2021-38507	The Opportunistic Encryption feature of HTTP2 (RFC 8164) allows a connection to be transparently upgraded to TLS while retaining the visual properties of an HTTP connection, including being same-origin with unencrypted connections on port 80. However, if a second encrypted port on the same IP address (e.g. port 8443) did not opt-in to opportunistic encryption; a network attacker could forward a connection from the browser to port 443 to port 8443, causing the browser to treat the content of port 8443 as same-origin with HTTP. This was resolved by disabling the Opportunistic Encryption feature, which had low usage. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.	6.5	More Details
CVE-2021-22565	An attacker could prematurely expire a verification code, making it unusable by the patient, making the patient unable to upload their TEKs to generate exposure notifications. We recommend upgrading the Exposure Notification server to V1.1.2 or greater.	6.5	More Details
CVE-2021-43536	Under certain circumstances, asynchronous functions could have caused a navigation to fail but expose the target URL. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38505	Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios. Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats; and Firefox before versions 94 and ESR 91.3 did not implement them. This could have caused sensitive data to be recorded to a user's Microsoft account. *This bug only affects Firefox for Windows 10+ with Cloud Clipboard enabled. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.	6.5	More Details
CVE-2021-23561	All versions of package comb are vulnerable to Prototype Pollution via the deepMerge() function.	6.5	More Details
CVE-2021-23663	All versions of package sey are vulnerable to Prototype Pollution via the deepmerge() function.	6.5	More Details
CVE-2021-38937	IBM PowerVM Hypervisor FW940, FW950, and FW1010 could allow an authenticated user to cause the system to crash using a specially crafted IBMi Hypervisor call. IBM X-Force ID: 210894.	6.5	More Details
CVE-2021-23700	All versions of package merge-deep2 are vulnerable to Prototype Pollution via the mergeDeep() function.	6.5	More Details
CVE-2021-23861	By executing a special command, an user with administrative rights can get access to extended debug functionality on the VRM allowing an impact on integrity or availability of the installed software. This issue also affects installations of the DIVAR IP and BVMS with VRM installed.	6.5	More Details
CVE-2021-42023	A vulnerability has been identified in ModelSim Simulation (All versions), Questa Simulation (All versions). The RSA white-box implementation in affected applications insufficiently protects the built-in private keys that are required to decrypt electronic intellectual property (IP) data in accordance with the IEEE 1735 recommended practice. This could allow a sophisticated attacker to discover the keys, bypassing the protection intended by the IEEE 1735 recommended practice.	6.5	More Details
CVE-2021-43528	Thunderbird unexpectedly enabled JavaScript in the composition area. The JavaScript execution context was limited to this area and did not receive chrome-level privileges, but could be used as a stepping stone to further an attack with other vulnerabilities. This vulnerability affects Thunderbird < 91.4.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37187	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords.	6.5	More Details
CVE-2021-37039	There is an Input verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause Bluetooth DoS.	6.5	More Details
CVE-2021-40007	There is an information leak vulnerability in eCNS280_TD V100R005C10SPC650. The vulnerability is caused by improper log output management. An attacker with the ability to access the log file of device may lead to information disclosure.	6.5	More Details
CVE-2021-4033	kimai2 is vulnerable to Cross-Site Request Forgery (CSRF)	6.5	More Details
CVE-2021-43797	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. Netty prior to version 4.1.71.Final skips control chars when they are present at the beginning / end of the header name. It should instead fail fast as these are not allowed by the spec and could lead to HTTP request smuggling. Failing to do the validation might cause netty to "sanitize" header names before it forward these to another remote system when used as proxy. This remote system can't see the invalid usage anymore, and therefore does not do the validation itself. Users should upgrade to version 4.1.71.Final.	6.5	More Details
CVE-2020-16155	The CPAN::Checksums package 2.12 for Perl does not uniquely define signed data.	6.5	More Details
CVE-2021-25516	An improper check or handling of exceptional conditions in Exynos baseband prior to SMR Dec-2021 Release 1 allows attackers to track locations.	6.4	More Details
CVE-2021-25518	An improper boundary check in secure_log of LDFW and BL31 prior to SMR Dec-2021 Release 1 allows arbitrary memory write and code execution.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42367	The Variation Swatches for WooCommerce WordPress plugin is vulnerable to Stored Cross-Site Scripting via several parameters found in the ~/includes/class-menu-page.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.1.1. Due to missing authorization checks on the tawcvs_save_settings function, low-level authenticated users such as subscribers can exploit this vulnerability.	6.4	More Details
CVE-2021-41029	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiWLM version 8.6.1 and below allows attacker to store malicious javascript code in the device and trigger it via crafted HTTP requests	6.4	More Details
CVE-2021-25511	An improper validation vulnerability in FilterProvider prior to SMR Dec-2021 Release 1 allows attackers to write arbitrary files via a path traversal vulnerability.	6.3	More Details
CVE-2021-26103	An insufficient verification of data authenticity vulnerability (CWE-345) in the user interface of FortiProxy verison 2.0.3 and below, 1.2.11 and below and FortiGate verison 7.0.0, 6.4.6 and below, 6.2.9 and below of SSL VPN portal may allow a remote, unauthenticated attacker to conduct a cross-site request forgery (CSRF) attack . Only SSL VPN in web mode or full mode are impacted by this vulnerability.	6.3	More Details
CVE-2021-38361	The .htaccess Redirect WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the link parameter found in the ~/htaccess-redirect.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.3.1.	6.1	More Details
CVE-2021-39308	The WooCommerce myghpay Payment Gateway WordPess plugin is vulnerable to Reflected Cross-Site Scripting via the clientref parameter found in the ~/processresponse.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.0.	6.1	More Details
CVE-2021-39309	The Parsian Bank Gateway for Woocommerce WordPress plugin is vulnerable to Reflected Cross-Site Scripting via and parameter due to a var_dump() on $_POST variables found in the ~/vendor/dpsoft/parsian-payment/sample/rollback-payment.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.	6.1	More Details
CVE-2021-39310	The Real WYSIWYG WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of PHP_SELF in the ~/real-wysiwyg.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.0.2.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3831	gnuboard5 is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-4107	yetiforcecrm is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-39311	The link-list-manager WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the category parameter found in the ~/llm.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.	6.1	More Details
CVE-2021-39313	The Simple Image Gallery WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the msg parameter found in the ~/simple-image-gallery.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.6.	6.1	More Details
CVE-2020-19042	Cross Site Scripting (XSS) vulnerability exists in zzcms 2019 XSS via a modify action in user/adv.php.	6.1	More Details
CVE-2021-39314	The WooCommerce EnvioPack WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the dataid parameter found in the ~/includes/functions.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.	6.1	More Details
CVE-2021-24955	The User Registration, Login Form, User Profile & Membership WordPress plugin before 3.2.3 does not escape the data parameter of the pp_get_forms_by_builder_type AJAX action before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-42050	An issue was discovered in AbanteCart before 1.3.2. It allows DOM Based XSS.	6.1	More Details
CVE-2021-4081	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-24954	The User Registration, Login Form, User Profile & Membership WordPress plugin before 3.2.3 does not sanitise and escape the ppress_cc_data parameter before outputting it back in an attribute of an admin dashboard page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36718	SYNEL - eharmonynew / Synel Reports - The attacker can log in to the system with default credentials and export a report of eharmony system with sensetive data (Employee name, Employee ID number, Working hours etc') The vulnerabilety has been addressed and fixed on version 11. Default credentials , Security miscommunication , Sensetive data exposure vulnerability in Synel Reports of SYNEL eharmonynew, Synel Reports allows an attacker to log into the system with default credentials. This issue affects: SYNEL eharmonynew, Synel Reports 8.0.2 version 11 and prior versions.	6.1	More Details
CVE-2021-4084	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-41697	A reflected Cross Site Scripting (XSS) vulnerability exists in Premiumdatingscript 4.2.7.7 via the aerror_description parameter in assets/sources/instagram.php script.	6.1	More Details
CVE-2021-24932	The Auto Featured Image (Auto Post Thumbnail) WordPress plugin before 3.9.3 does not sanitise and escape the post_id parameter before outputting back in an admin page within a JS block, leading to a Reflected Cross-Site Scripting issue.	6.1	More Details
CVE-2021-43544	When receiving a URL through a SEND intent, Firefox would have searched for the text, but subsequent usages of the address bar might have caused the URL to load unintentionally, which could lead to XSS and spoofing attacks. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 95.	6.1	More Details
CVE-2021-43543	Documents loaded with the CSP sandbox directive could have escaped the sandbox's script restriction by embedding additional content. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95.	6.1	More Details
CVE-2021-43532	The 'Copy Image Link' context menu action would copy the final image URL after redirects. By embedding an image that triggered authentication flows - in conjunction with a Content Security Policy that stopped a redirection chain in the middle - the final image URL could be one that contained an authentication token used to takeover a user account. If a website tricked a user into copy and pasting the image link back to the page, the page would be able to steal the authentication tokens. This was fixed by making the action return the original URL, before any redirects. This vulnerability affects Firefox < 94.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43530	A Universal XSS vulnerability was present in Firefox for Android resulting from improper sanitization when processing a URL scanned from a QR code. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94.	6.1	More Details
CVE-2021-40882	A Cross Site Scripting (XSS) vulnerability exists in Piwigo 11.5.0 via the system album name and description of the location.	6.1	More Details
CVE-2021-36720	PineApp - Mail Secure - Attacker sending a request to :/blocking.php?url=<script>alert(1)</script> and stealing cookies .	6.1	More Details
CVE-2021-36188	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows attacker to execute unauthorized code or commands via crafted GET parameters in requests to login and error handlers	6.1	More Details
CVE-2021-42063	A security vulnerability has been discovered in the SAP Knowledge Warehouse - versions 7.30, 7.31, 7.40, 7.50. The usage of one SAP KW component within a Web browser enables unauthorized attackers to conduct XSS attacks, which might lead to disclose sensitive data.	6.1	More Details
CVE-2018-10228	Cross-site scripting (XSS) vulnerability in /application/controller/admin/theme.php in LimeSurvey 3.6.2+180406 allows remote attackers to inject arbitrary web script or HTML via the changes_cp parameter to the index.php/admin/themes/sa/templatesavechanges URI.	6.1	More Details
CVE-2021-25512	An improper validation vulnerability in telephony prior to SMR Dec-2021 Release 1 allows attackers to launch certain activities.	6.1	More Details
CVE-2021-43063	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiWeb version 6.4.1 and 6.4.0, version 6.3.15 and below, version 6.2.6 and below allows attacker to execute unauthorized code or commands via crafted HTTP GET requests to the login webpage.	6.1	More Details
CVE-2021-4108	snipe-it is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-41015	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests to SAML login handler	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4050	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-31850	A denial-of-service vulnerability in Database Security (DBS) prior to 4.8.4 allows a remote authenticated administrator to trigger a denial-of-service attack against the DBS server. The configuration of Archiving through the User interface incorrectly allowed the creation of directories and files in Windows system directories and other locations where sensitive data could be overwritten. The former could lead to a DoS, whilst the latter could lead to data destruction on the DBS server.	6.1	More Details
CVE-2021-3370	DouPHP v1.6 was discovered to contain a cross-site scripting (XSS) vulnerability via /admin/cloud.php.	6.1	More Details
CVE-2020-22421	74CMS v6.0.4 was discovered to contain a cross-site scripting (XSS) vulnerability via /index.php?m=&c=help&a=help_list&key.	6.1	More Details
CVE-2021-3829	openwhyd is vulnerable to URL Redirection to Untrusted Site	6.1	More Details
CVE-2021-20137	A reflected cross-site scripting vulnerability exists in the url parameter of the /cgi-bin/luci/site_access/ page on the Gryphon Tower router's web interface. An attacker could exploit this issue by tricking a user into following a specially crafted link, granting the attacker javascript execution in the context of the victim's browser.	6.1	More Details
CVE-2021-24756	The WP System Log WordPress plugin before 1.0.21 does not sanitise, validate and escape the IP address retrieved from login requests before outputting them in the admin dashboard, which could allow unauthenticated attacker to perform Cross-Site Scripting attacks against admins viewing the logs.	6.1	More Details
CVE-2021-39318	The H5P CSS Editor WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the h5p-css-file parameter found in the ~/h5p-css-editor.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.	6.1	More Details
CVE-2021-39315	The Magic Post Voice WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the ids parameter found in the ~/inc/admin/main.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39319	The duoFAQ - Responsive, Flat, Simple FAQ WordPess plugin is vulnerable to Reflected Cross-Site Scripting via the msg parameter found in the ~/duogeek/duogeek-panel.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.4.8.	6.1	More Details
CVE-2021-24925	The Modern Events Calendar Lite WordPress plugin before 6.1.5 does not sanitise and escape the current_month_divider parameter of its mec_list_load_more AJAX call (available to both unauthenticated and authenticated users) before outputting it back in the response, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-24792	The Shiny Buttons WordPress plugin through 1.1.0 does not have any authorisation and CSRF in place when saving a template (wpbtn_save_template function hooked to the init action), nor sanitise and escape them before outputting them in the admin dashboard, which allow unauthenticated users to add a malicious template and lead to Stored Cross-Site Scripting issues.	6.1	More Details
CVE-2021-25520	Insecure caller check and input validation vulnerabilities in SearchKeyword deeplink logic prior to Samsung Internet 16.0.2 allows unstrusted applications to execute script codes in Samsung Internet.	5.9	More Details
CVE-2021-39937	A collision in access memoization logic in all versions of GitLab CE/EE before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, leads to potential elevated privileges in groups and projects under rare circumstances	5.9	More Details
CVE-2020-4496	The IBM Spectrum Protect Plus 10.1.0.0 through 10.1.8.x server connection to an IBM Spectrum Protect Plus workload agent is subject to a man-in-the-middle attack due to improper certificate validation. IBM X-Force ID: 182046.	5.9	More Details
CVE-2021-37861	Mattermost 6.0.2 and earlier fails to sufficiently sanitize user's password in audit logs when user creation fails.	5.8	More Details
CVE-2021-44017	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Image.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted TIF files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15111)	5.5	More Details
CVE-2021-3836	dbeaver is vulnerable to Improper Restriction of XML External Entity Reference	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44010	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing TIFF files. An attacker could leverage this vulnerability to leak information in the context of the current process.	5.5	More Details
CVE-2021-38926	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to gain privileges due to allowing modification of columns of existing tasks. IBM X-Force ID: 210321.	5.5	More Details
CVE-2021-39048	IBM Spectrum Protect Client 7.1 and 8.1 is vulnerable to a stack based buffer overflow, caused by improper bounds checking. A local attacker could exploit this vulnerability and cause a denial of service. IBM X-Force ID: 214438.	5.5	More Details
CVE-2021-38901	IBM Spectrum Protect Operations Center 7.1, under special configurations, could allow a local user to obtain highly sensitive information. IBM X-Force ID: 209610.	5.5	More Details
CVE-2021-44009	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing TIFF files. An attacker could leverage this vulnerability to leak information in the context of the current process.	5.5	More Details
CVE-2021-44012	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Jt1001.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15102)	5.5	More Details
CVE-2021-44003	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll is vulnerable to use of uninitialized memory while parsing user supplied TIFF files. This could allow an attacker to cause a denial-of-service condition.	5.5	More Details
CVE-2021-36190	A unintended proxy or intermediary ('confused deputy') in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows an unauthenticated attacker to access protected hosts via crafted HTTP requests.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44004	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing TIFF files. An attacker could leverage this vulnerability to leak information in the context of the current process.	5.5	More Details
CVE-2021-44011	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Jt1001.dll is vulnerable to an out of bounds read past the end of an allocated buffer while parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15101)	5.5	More Details
CVE-2021-44007	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll contains an off-by-one error in the heap while parsing specially crafted TIFF files. This could allow an attacker to cause a denial-of-service condition.	5.5	More Details
CVE-2021-44008	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing TIFF files. An attacker could leverage this vulnerability to leak information in the context of the current process.	5.5	More Details
CVE-2021-44015	A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The VCRUNTIME140.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted CGM files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15109)	5.5	More Details
CVE-2021-24855	The Display Post Metadata WordPress plugin before 1.5.0 adds a shortcode to print out custom fields, however their content is not sanitised or escaped which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2021-41030	An authentication bypass by capture-replay vulnerability [CWE-294] in FortiClient EMS versions 7.0.1 and below and 6.4.4 and below may allow an unauthenticated attacker to impersonate an existing user by intercepting and re-using valid SAML authentication messages.	5.4	More Details
CVE-2021-24817	The Ultimate NoFollow WordPress plugin through 1.4.8 does not sanitise and escape the href attribute of its shortcodes, allowing users with a role as low as contributor to perform Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44043	An issue was discovered in UiPath App Studio 21.4.4. There is a persistent XSS vulnerability in the file-upload functionality for uploading icons when attempting to create new Apps. An attacker with minimal privileges in the application can build their own App and upload a malicious file containing an XSS payload, by uploading an arbitrary file and modifying the MIME type in a subsequent HTTP request. This then allows the file to be stored and retrieved from the server by other users in the same organization.	5.4	More Details
CVE-2021-43068	A improper authentication in Fortinet FortiAuthenticator version 6.4.0 allows user to bypass the second factor of authentication via a RADIUS login portal.	5.4	More Details
CVE-2020-19683	A Cross Site Scripting (XSS) exists in ZZZCMS V1.7.1 via an editfile action in save.php.	5.4	More Details
CVE-2021-39054	IBM Spectrum Copy Data Management 2.2.13 and earlier could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 214525.	5.4	More Details
CVE-2021-24871	The Get Custom Field Values WordPress plugin before 4.0.1 does not escape custom fields before outputting them in the page, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2021-42051	An issue was discovered in AbanteCart before 1.3.2. Any low-privileged user with file-upload permissions can upload a malicious SVG document that contains an XSS payload.	5.4	More Details
CVE-2021-42061	SAP BusinessObjects Business Intelligence Platform (Web Intelligence) - version 420, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. This allows a low privileged attacker to retrieve some data from the victim but will never be able to modify the document and publish these modifications to the server. It impacts the "Quick Prompt" workflow.	5.4	More Details
CVE-2021-4097	phpservermon is vulnerable to Improper Neutralization of CRLF Sequences	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42752	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiWLM version 8.6.1 and below allows attacker to execute malicious javascript code on victim's host via crafted HTTP requests	5.4	More Details
CVE-2021-34426	A vulnerability was discovered in the Keybase Client for Windows before version 5.6.0 when a user executed the "keybase git lfs-config" command on the command-line. In versions prior to 5.6.0, a malicious actor with write access to a user\'s Git repository could leverage this vulnerability to potentially execute arbitrary Windows commands on a user\'s local system.	5.3	More Details
CVE-2021-44937	glFusion CMS v1.7.9 is affected by an arbitrary user registration vulnerability in /public_html/users.php. An attacker can register with the mailbox of any user. When users want to register, they will find that the mailbox has been occupied.	5.3	More Details
CVE-2021-39915	Improper access control in the GraphQL API in GitLab CE/EE affecting all versions starting from 13.0 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an attacker to see the names of project access tokens on arbitrary projects	5.3	More Details
CVE-2021-37093	There is a Improper Access Control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to attackers steal short messages.	5.3	More Details
CVE-2021-25510	An improper validation vulnerability in FilterProvider prior to SMR Dec-2021 Release 1 allows local arbitrary code execution.	5.3	More Details
CVE-2021-32591	A missing cryptographic steps vulnerability in the function that encrypts users' LDAP and RADIUS credentials in FortiSandbox before 4.0.1, FortiWeb before 6.3.12, FortiADC before 6.2.1, FortiMail 7.0.1 and earlier may allow an attacker in possession of the password store to compromise the confidentiality of the encrypted secrets.	5.3	More Details
CVE-2021-41309	Affected versions of Atlassian Jira Server and Data Center allow a user who has had their Jira Service Management access revoked to export audit logs of another user's Jira Service Management project via a Broken Authentication vulnerability in the /plugins/servlet/audit/resource endpoint. The affected versions of Jira Server and Data Center are before version 8.19.1.	5.3	More Details
CVE-2021-25522	Insecure storage of sensitive information vulnerability in Smart Capture prior to version 4.8.02.10 allows attacker to access victim's captured images without permission.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43808	Laravel is a web application framework. Laravel prior to versions 8.75.0, 7.30.6, and 6.20.42 contain a possible cross-site scripting (XSS) vulnerability in the Blade templating engine. A broken HTML element may be clicked and the user taken to another location in their browser due to XSS. This is due to the user being able to guess the parent placeholder SHA-1 hash by trying common names of sections. If the parent template contains an exploitable HTML structure an XSS vulnerability can be exposed. This vulnerability has been patched in versions 8.75.0, 7.30.6, and 6.20.42 by determining the parent placeholder at runtime and using a random hash that is unique to each request.	5.3	More Details
CVE-2021-41013	An improper access control vulnerability [CWE-284] in FortiWeb versions 6.4.1 and below and 6.3.15 and below in the Report Browse section of Log & Report may allow an unauthorized and unauthenticated user to access the Log reports via their URLs.	5.3	More Details
CVE-2021-43410	Apache Airavata Django Portal allows CRLF log injection because of lack of escaping log statements. In particular, some HTTP request parameters are logged without first being escaped. Versions affected: master branch before commit 3c5d8c7 [1] of airavata-django-portal [1] https://github.com/apache/airavata-django-portal/commit/3c5d8c72bfc3eb0af8693a655a5d60f9273f8170	5.3	More Details
CVE-2021-44848	In Cibele Thinfinity VirtualUI before 3.0, /changePassword returns different responses for invalid authentication requests depending on whether the username exists.	5.3	More Details
CVE-2021-44155	An issue was discovered in /goform/login_process in Reprise RLM 14.2. When an attacker attempts to login, the response if a username is valid includes Login Failed, but does not include this string if the username is invalid. This allows an attacker to enumerate valid users.	5.3	More Details
CVE-2021-23860	An error in a page handler of the VRM may lead to a reflected cross site scripting (XSS) in the web-based interface. To exploit this vulnerability an attack must be able to modify the HTTP header that is sent. This issue also affects installations of the DIVAR IP and BVMS with VRM installed.	5.0	More Details
CVE-2021-40858	Auerswald COMpact 5500R devices before 8.2B allow Arbitrary File Disclosure. A sub-admin can read the cleartext Admin password via the fileName=../../etc/passwd substring.	4.9	More Details
CVE-2021-36911	Stored Cross-Site Scripting (XSS) vulnerability discovered in WordPress Comment Engine Pro plugin (versions <= 1.0), could be exploited by users with Editor or higher role.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24972	The Pixel Cat WordPress plugin before 2.6.3 does not escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	4.8	More Details
CVE-2021-41836	The Fathom Analytics WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and escaping via the $site_id parameter found in the ~/fathom-analytics.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 3.0.4. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	4.8	More Details
CVE-2021-31747	Missing SSL Certificate Validation issue exists in Pluck 4.7.15 in update_applet.php, which could lead to man-in-the-middle attacks.	4.8	More Details
CVE-2021-24896	The Caldera Forms WordPress plugin before 1.9.5 does not sanitise and escape the Form Name before outputting it in attributes, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-4038	Cross Site Scripting (XSS) vulnerability in McAfee Network Security Manager (NSM) prior to 10.1 Minor 7 allows a remote authenticated administrator to embed a XSS in the administrator interface via specially crafted custom rules containing HTML. NSM did not correctly sanitize custom rule content in all scenarios.	4.8	More Details
CVE-2021-24771	The Inspirational Quote Rotator WordPress plugin through 1.0.0 does not sanitize and escape some of its quote fields when adding/editing a quote as admin, leading to Stored Cross-Site scripting issues when the quote is output in the "Quotes list" even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24782	The Flex Local Fonts WordPress plugin through 1.0.0 does not escape the Class Name field when adding a font, which could allow hight privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24705	The NEX-Forms WordPress plugin before 8.4.3 does not have CSRF checks in place when editing a form, and does not escape some of its settings as well as form fields before outputting them in attributes. This could allow attackers to make a logged in admin edit arbitrary forms with Cross-Site Scripting payloads in them	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42549	Insufficient Input Validation in the search functionality of Wordpress plugin Lets-Box prior to 1.15.3 allows unauthenticated user to craft a reflected Cross-Site Scripting attack.	4.7	More Details
CVE-2021-34425	The Zoom Client for Meetings before version 5.7.3 (for Android, iOS, Linux, macOS, and Windows) contain a server side request forgery vulnerability in the chat\'s "link preview" functionality. In versions prior to 5.7.3, if a user were to enable the chat\'s "link preview" feature, a malicious actor could trick the user into potentially sending arbitrary HTTP GET requests to URLs that the actor cannot reach directly.	4.7	More Details
CVE-2021-42548	Insufficient Input Validation in the search functionality of Wordpress plugin Share-one-Drive prior to 1.15.3 allows unauthenticated user to craft a reflected Cross-Site Scripting attack.	4.7	More Details
CVE-2021-42547	Insufficient Input Validation in the search functionality of Wordpress plugin Out-of-the-Box prior to 1.20.3 allows unauthenticated user to craft a reflected Cross-Site Scripting attack.	4.7	More Details
CVE-2021-42546	Insufficient Input Validation in the search functionality of Wordpress plugin Use-Your-Drive prior to 1.18.3 allows unauthenticated user to craft a reflected Cross-Site Scripting attack.	4.7	More Details
CVE-2021-41246	Express OpenID Connect is express JS middleware implementing sign on for Express web apps using OpenID Connect. Versions before and including `2.5.1` do not regenerate the session id and session cookie when user logs in. This behavior opens up the application to various session fixation vulnerabilities. Versions `2.5.2` contains a patch for this issue.	4.6	More Details
CVE-2021-42066	SAP Business One - version 10.0, allows an admin user to view DB password in plain text over the network, which should otherwise be encrypted. For an attacker to discover vulnerable function in-depth application knowledge is required, but once exploited the attacker may be able to completely compromise confidentiality, integrity, and availability of the application.	4.4	More Details
CVE-2021-36721	Sysaid API User Enumeration - Attacker sending requests to specific api path without any authorization before 21.3.60 version could get users names from the LDAP server.	4.4	More Details
CVE-2021-43204	A improper control of a resource through its lifetime in Fortinet FortiClientWindows version 6.4.1 and 6.4.0, version 6.2.9 and below, version 6.0.10 and below allows attacker to cause a complete denial of service of its components via changes of directory access permissions.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39919	In all versions of GitLab CE/EE starting version 14.0 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, the reset password token and new user email token are accidentally logged which may lead to information disclosure.	4.4	More Details
CVE-2021-44942	glFusion CMS 1.7.9 is affected by a Cross Site Request Forgery (CSRF) vulnerability in /public_html/admin/plugins/bad_behavior2/blacklist.php. Using the CSRF vulnerability to trick the administrator to click, an attacker can add a blacklist.	4.3	More Details
CVE-2021-43827	discourse-footnote is a library providing footnotes for posts in Discourse. ### Impact When posting an inline footnote wrapped in `<a>` tags (e.g. `<a>^[footnote]</a>`, the resulting rendered HTML would include a nested `<a>`, which is stripped by Nokogiri because it is not valid. This then caused a javascript error on topic pages because we were looking for an `<a>` element inside the footnote reference span and getting its ID, and because it did not exist we got a null reference error in javascript. Users are advised to update to version 0.2. As a workaround editing offending posts from the rails console or the database console for self-hosters, or disabling the plugin in the admin panel can mitigate this issue.	4.3	More Details
CVE-2021-43813	Grafana is an open-source platform for monitoring and observability. Grafana prior to versions 8.3.2 and 7.5.12 contains a directory traversal vulnerability for fully lowercase or fully uppercase .md files. The vulnerability is limited in scope, and only allows access to files with the extension .md to authenticated users only. Grafana Cloud instances have not been affected by the vulnerability. Users should upgrade to patched versions 8.3.2 or 7.5.12. For users who cannot upgrade, running a reverse proxy in front of Grafana that normalizes the PATH of the request will mitigate the vulnerability. The proxy will have to also be able to handle url encoded paths. Alternatively, for fully lowercase or fully uppercase .md files, users can block /api/plugins/.*/markdown/.* without losing any functionality beyond inlined plugin help text.	4.3	More Details
CVE-2021-24859	The User Meta Shortcodes WordPress plugin through 0.5 registers a shortcode that allows any user with a role as low as contributor to access other users metadata by specifying the user login as a parameter. This makes the WP instance vulnerable to data extrafiltration, including password hashes	4.3	More Details
CVE-2021-24819	The Page/Post Content Shortcode WordPress plugin through 1.0 does not have proper authorisation in place, allowing users with a role as low as contributor to access draft/private/password protected/trashed posts/pages they should not be allowed to, including posts created by other users such as admins and editors.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24818	The WP Limits WordPress plugin through 1.0 does not have CSRF check when saving its settings, allowing attacker to make a logged in admin change them, which could make the blog unstable by setting low values	4.3	More Details
CVE-2021-24790	The Contact Form Advanced Database WordPress plugin through 1.0.8 does not have any authorisation as well as CSRF checks in its delete_cf7_data and export_cf7_data AJAX actions, available to any authenticated users, which could allow users with a role as low as subscriber to call them. The delete_cf7_data would lead to arbitrary metadata deletion, as well as PHP Object Injection if a suitable gadget chain is present in another plugin, as user data is passed to the maybe_unserialize() function without being first validated.	4.3	More Details
CVE-2021-24780	The Single Post Exporter WordPress plugin through 1.1.1 does not have CSRF checks when saving its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and give access to the export feature to any role such as subscriber. Subscriber users would then be able to export an arbitrary post/page (such as private and password protected) via a direct URL	4.3	More Details
CVE-2021-4092	yetiforcecrm is vulnerable to Cross-Site Request Forgery (CSRF)	4.3	More Details
CVE-2021-43815	Grafana is an open-source platform for monitoring and observability. Grafana prior to versions 8.3.2 and 7.5.12 has a directory traversal for arbitrary .csv files. It only affects instances that have the developer testing tool called TestData DB data source enabled and configured. The vulnerability is limited in scope, and only allows access to files with the extension .csv to authenticated users only. Grafana Cloud instances have not been affected by the vulnerability. Versions 8.3.2 and 7.5.12 contain a patch for this issue. There is a workaround available for users who cannot upgrade. Running a reverse proxy in front of Grafana that normalizes the PATH of the request will mitigate the vulnerability. The proxy will have to also be able to handle url encoded paths.	4.3	More Details
CVE-2021-4089	snipe-it is vulnerable to Improper Access Control	4.3	More Details
CVE-2021-40834	A user interface overlay vulnerability was discovered in F-secure SAFE Browser for Android. When user click on a specially crafted seemingly legitimate URL SAFE browser goes into full screen and hides the user interface. A remote attacker can leverage this to perform spoofing attack.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4082	pimcore is vulnerable to Cross-Site Request Forgery (CSRF)	4.3	More Details
CVE-2021-36167	An improper authorization vulnerabiltiy [CWE-285] in FortiClient Windows versions 7.0.0 and 6.4.6 and below and 6.2.8 and below may allow an unauthenticated attacker to bypass the webfilter control via modifying the session-id paramater.	4.3	More Details
CVE-2021-43546	It was possible to recreate previous cursor spoofing attacks against users with a zoomed native cursor. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95.	4.3	More Details
CVE-2021-43538	By misusing a race in our notification code, an attacker could have forcefully hidden the notification for pages that had received full screen and pointer lock access, which could have been used for spoofing attacks. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95.	4.3	More Details
CVE-2021-43533	When parsing internationalized domain names, high bits of the characters in the URLs were sometimes stripped, resulting in inconsistencies that could lead to user confusion or attacks such as phishing. This vulnerability affects Firefox < 94.	4.3	More Details
CVE-2021-43531	When a user loaded a Web Extensions context menu, the Web Extension could access the post-redirect URL of the element clicked. If the Web Extension lacked the WebRequest permission for the hosts involved in the redirect, this would be a same-origin-violation leaking data the Web Extension should have access to. This was fixed to provide the pre-redirect URL. This is related to CVE-2021-43532 but in the context of Web Extensions. This vulnerability affects Firefox < 94.	4.3	More Details
CVE-2021-38509	Due to an unusual sequence of attacker-controlled events, a Javascript alert() dialog with arbitrary (although unstyled) contents could be displayed over top an uncontrolled webpage of the attacker's choosing. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.	4.3	More Details
CVE-2021-38506	Through a series of navigations, Firefox could have entered fullscreen mode without notification or warning to the user. This could lead to spoofing attacks on the browser UI including phishing. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24836	The Temporary Login Without Password WordPress plugin before 1.7.1 does not have authorisation and CSRF checks when updating its settings, which could allows any logged-in users, such as subscribers to update them	4.3	More Details
CVE-2021-38508	By displaying a form validity message in the correct location at the same time as a permission prompt (such as for geolocation), the validity message could have obscured the prompt, resulting in the user potentially being tricked into granting the permission. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.	4.3	More Details
CVE-2021-39934	Improper access control allows any project member to retrieve the service desk email address in GitLab CE/EE versions starting 12.10 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2.	4.3	More Details
CVE-2021-39916	Lack of an access control check in the External Status Check feature allowed any authenticated user to retrieve the configuration of any External Status Check in GitLab EE starting from 14.1 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2.	4.3	More Details
CVE-2021-39917	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.9 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. A regular expression related to quick actions features was susceptible to catastrophic backtracking that could cause a DOS attack.	4.3	More Details
CVE-2021-43064	A url redirection to untrusted site ('open redirect') in Fortinet FortiWeb version 6.4.1 and 6.4.0, version 6.3.15 and below, version 6.2.6 and below allows attacker to use the device as a proxy and reach external or protected hosts via redirection handlers.	4.3	More Details
CVE-2021-39930	Missing authorization in GitLab EE versions between 12.4 and 14.3.6, between 14.4.0 and 14.4.4, and between 14.5.0 and 14.5.2 allowed an attacker to access a user's custom project and group templates	4.3	More Details
CVE-2021-39940	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.2 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. GitLab Maven Package registry is vulnerable to a regular expression denial of service when a specifically crafted string is sent.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39932	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.0 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. Using large payloads, the diff feature could be used to trigger high load time for users reviewing code changes.	4.3	More Details
CVE-2021-39933	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.10 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. A regular expression used for handling user input (notes, comments, etc) was susceptible to catastrophic backtracking that could cause a DOS attack.	4.3	More Details
CVE-2021-36195	Multiple command injection vulnerabilities in the command line interpreter of FortiWeb versions 6.4.1, 6.4.0, 6.3.0 through 6.3.15, 6.2.0 through 6.2.6, and 6.1.0 through 6.1.2 may allow an authenticated attacker to execute arbitrary commands on the underlying system shell via specially crafted command arguments.	4.2	More Details
CVE-2021-36169	A Hidden Functionality in Fortinet FortiOS 7.x before 7.0.1, FortiOS 6.4.x before 6.4.7 allows attacker to Execute unauthorized code or commands via specific hex read/write operations.	4.2	More Details
CVE-2021-36191	A url redirection to untrusted site ('open redirect') in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows attacker to use the device as proxy via crafted GET parameters in requests to error handlers	4.1	More Details
CVE-2021-25523	Insecure storage of device information in Samsung Dialer prior to version 12.7.05.24 allows attacker to get Samsung Account ID.	4.0	More Details
CVE-2021-25524	Insecure storage of device information in Contacts prior to version 12.7.05.24 allows attacker to get Samsung Account ID.	4.0	More Details
CVE-2021-25515	An improper usage of implicit intent in SemRewardManager prior to SMR Dec-2021 Release 1 allows attackers to access BSSID.	4.0	More Details
CVE-2021-25519	An improper access control vulnerability in CPLC prior to SMR Dec-2021 Release 1 allows local attackers to access CPLC information without permission.	4.0	More Details
CVE-2021-25521	Insecure caller check in sharevia deeplink logic prior to Samsung Internet 16.0.2 allows unstrusted applications to get current tab URL in Samsung Internet.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25526	Intent redirection vulnerability in Samsung Blockchain Wallet prior to version 1.3.02.8 allows attacker to execute privileged action.	4.0	More Details
CVE-2021-25527	Improper export of Android application components vulnerability in Samsung Pay (India only) prior to version 4.1.77 allows attacker to access Bill Pay and Recharge menu without authentication.	3.8	More Details
CVE-2021-39941	An information disclosure vulnerability in GitLab CE/EE versions 12.0 to 14.3.6, 14.4 to 14.4.4, and 14.5 to 14.5.2 allowed non-project members to see the default branch name for projects that restrict access to the repository to project members	3.7	More Details
CVE-2021-39936	Improper access control in GitLab CE/EE affecting all versions starting from 10.7 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an attacker in possession of a deploy token to access a project's disabled wiki.	3.5	More Details
CVE-2021-25514	An improper intent redirection handling in Tags prior to SMR Dec-2021 Release 1 allows attackers to access sensitive information.	3.3	More Details
CVE-2021-44448	A vulnerability has been identified in JT Utilities (All versions < V13.0.3.0), JTTK (All versions < V11.0.3.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14843, ZDI-CAN-15051)	3.3	More Details
CVE-2021-42070	When a user opens manipulated Jupiter Tessellation (.jt) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9.0, the application crashes and becomes temporarily unavailable to the user until restart of the application	3.3	More Details
CVE-2021-42069	When a user opens manipulated Tagged Image File Format (.tif) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9.0, the application crashes and becomes temporarily unavailable to the user until restart of the application	3.3	More Details
CVE-2021-42068	When a user opens a manipulated GIF (.gif) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9.0, the application crashes and becomes temporarily unavailable to the user until restart of the application.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44444	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15052)	3.3	More Details
CVE-2021-44431	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14841)	3.3	More Details
CVE-2021-44436	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14905)	3.3	More Details
CVE-2021-39918	Incorrect Authorization in GitLab EE affecting all versions starting from 11.1 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows a user to add comments to a vulnerability which cannot be accessed.	3.1	More Details
CVE-2021-39931	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.11 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. Under specific condition an unauthorised project member was allowed to delete a protected branches due to a business logic error.	3.1	More Details
CVE-2021-39938	A vulnerable regular expression pattern in GitLab CE/EE since version 8.15 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an attacker to cause uncontrolled resource consumption leading to Denial of Service via specially crafted deploy Slash commands	3.1	More Details
CVE-2018-25022	The Onion module in toxcore before 0.2.2 doesn't restrict which packets can be onion-routed, which allows a remote attacker to discover a target user's IP address (when knowing only their Tox Id) by positioning themselves close to target's Tox Id in the DHT for the target to establish an onion connection with the attacker, guessing the target's DHT public key and creating a DHT node with public key close to it, and finally onion-routing a NAT Ping Request to the target, requesting it to ping the just created DHT node.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39945	Improper access control in the GitLab CE/EE API affecting all versions starting from 9.4 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an author of a Merge Request to approve the Merge Request even after having their project access revoked	2.7	More Details
CVE-2021-39910	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.6 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. GitLab was vulnerable to HTML Injection through the Swagger UI feature.	2.6	More Details
CVE-2021-25513	An improper privilege management vulnerability in Apps Edge application prior to SMR Dec-2021 Release 1 allows unauthorized access to some device data on the lockscreen.	2.4	More Details
CVE-2021-25525	Improper check or handling of exception conditions vulnerability in Samsung Pay (US only) prior to version 4.0.65 allows attacker to use NFC without user recognition.	2.0	More Details
CVE-2021-44948	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-44942. Reason: This candidate is a duplicate of CVE-2021-44942. Notes: All CVE users should reference CVE-2021-44942 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details