SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 November 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-2021-34795	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2021-40112	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40113	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2021-40358	A vulnerability has been identified in SIMATIC PCS 7 V8.2 (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3 UC04), SIMATIC PCS 7 V9.1 (All versions < V9.1 SP1), SIMATIC WinCC V15 and earlier (All versions < V15 SP1 Update 7), SIMATIC WinCC V16 (All versions < V16 Update 5), SIMATIC WinCC V17 (All versions < V17 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 19), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). Legitimate file operations on the web server of 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, write or delete unexpected critical files.	9.9	More Details
CVE-2021-20700	Buffer overflow vulnerability in the Disk Agent CLUSTERPRO X 4.3 for Windows and earlier, EXPRESSCLUSTER X 4.3 for Windows and earlier, CLUSTERPRO X 4.3 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 4.3 SingleServerSafe for Windows and earlier allows attacker to remote code execution via a network.	9.8	More Details
CVE-2020-22226	Stivasoft (Phpjabbers) Fundraising Script v1.0 was discovered to contain a SQL injection vulnerability via the pjActionSetAmount function.	9.8	More Details
CVE-2021-42371	lpar2rrd is a hardcoded system account in XoruX LPAR2RRD and STOR2RRD before 7.30.	9.8	More Details
CVE-2021-42077	PHP Event Calendar before 2021-09-03 allows SQL injection, as demonstrated by the /server/ajax/user_manager.php username parameter. This can be used to execute SQL statements directly on the database, allowing an adversary in some cases to completely compromise the database system. It can also be used to bypass the login form.	9.8	More Details
CVE-2021-34684	Hitachi Vantara Pentaho Business Analytics through 9.1 allows an unauthenticated user to execute arbitrary SQL queries on any Pentaho data source and thus retrieve data from the related databases, as demonstrated by an api/repos/dashboards/editor URI.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22225	Stivasoft (Phpjabbers) Fundraising Script v1.0 was discovered to contain a SQL injection vulnerability via the pjActionLoadForm function.	9.8	More Details
CVE-2021-25979	Apostrophe CMS versions prior to 3.3.1 did not invalidate existing login sessions when disabling a user account or changing the password, creating a situation in which a device compromised by a third party could not be locked out by those means. As a mitigation for older releases the user account in question can be archived (3.x) or moved to the trash (2.x and earlier) which does disable the existing session.	9.8	More Details
CVE-2020-22223	Stivasoft (Phpjabbers) Fundraising Script v1.0 was discovered to contain a SQL injection vulnerability via the pjActionLoad function.	9.8	More Details
CVE-2021-42837	An issue was discovered in Talend Data Catalog before 7.3-20210930. After setting up SAML/OAuth, authentication is not correctly enforced on the native login page. Any valid user from the SAML/OAuth provider can be used as the username with an arbitrary password, and login will succeed.	9.8	More Details
CVE-2021-35368	OWASP ModSecurity Core Rule Set 3.1.x before 3.1.2, 3.2.x before 3.2.1, and 3.3.x before 3.3.2 is affected by a Request Body Bypass via a trailing pathname.	9.8	More Details
CVE-2021-42670	A SQL injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the id parameter to the announcements_student.php web page. As a result a malicious user can extract sensitive data from the web server and in some cases use this vulnerability in order to get a remote code execution on the remote web server.	9.8	More Details
CVE-2021-42669	A file upload vulnerability exists in Sourcecodester Engineers Online Portal in PHP via dashboard_teacher.php, which allows changing the avatar through teacher_avatar.php. Once an avatar gets uploaded it is getting uploaded to the /admin/uploads/ directory, and is accessible by all users. By uploading a php webshell containing "<?php system($_GET["cmd"]); ?>" the attacker can execute commands on the web server with - /admin/uploads/php-webshell?cmd=id.	9.8	More Details
CVE-2021-42668	A SQL Injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the id parameter in the my_classmates.php web page.. As a result, an attacker can extract sensitive data from the web server and in some cases can use this vulnerability in order to get a remote code execution on the remote web server.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42667	A SQL Injection vulnerability exists in Sourcecodester Online Event Booking and Reservation System in PHP in event-management/views. An attacker can leverage this vulnerability in order to manipulate the sql query performed. As a result he can extract sensitive data from the web server and in some cases he can use this vulnerability in order to get a remote code execution on the remote web server.	9.8	More Details
CVE-2021-30132	Cloudera Manager 7.2.4 has Incorrect Access Control, allowing Escalation of Privileges.	9.8	More Details
CVE-2021-28023	Arbitrary file upload in Service import feature in ServiceTonic Helpdesk software version < 9.0.35937 allows a malicious user to execute JSP code by uploading a zip that extracts files in relative paths.	9.8	More Details
CVE-2021-42237	Sitecore XP 7.5 Initial Release to Sitecore XP 8.2 Update-7 is vulnerable to an insecure deserialization attack where it is possible to achieve remote command execution on the machine. No authentication or special configuration is required to exploit this vulnerability.	9.8	More Details
CVE-2021-43185	JetBrains YouTrack before 2021.3.23639 is vulnerable to Host header injection.	9.8	More Details
CVE-2021-43571	The verify function in the Stark Bank Node.js ECDSA library (ecdsa-node) 1.1.2 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages.	9.8	More Details
CVE-2021-43570	The verify function in the Stark Bank Java ECDSA library (ecdsa-java) 1.0.0 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages.	9.8	More Details
CVE-2021-43569	The verify function in the Stark Bank .NET ECDSA library (ecdsa-dotnet) 1.3.1 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages.	9.8	More Details
CVE-2021-43568	The verify function in the Stark Bank Elixir ECDSA library (ecdsa-elixir) 1.0.0 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages.	9.8	More Details
CVE-2021-43200	In JetBrains TeamCity before 2021.1.2, permission checks in the Agent Push functionality were insufficient.	9.8	More Details
CVE-2021-43193	In JetBrains TeamCity before 2021.1.2, remote code execution via the agent push functionality is possible.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43183	In JetBrains Hub before 2021.1.13690, the authentication throttling mechanism could be bypassed.	9.8	More Details
CVE-2021-28024	Unauthorized system access in the login form in ServiceTonic Helpdesk software version < 9.0.35937 allows attacker to login without using a password.	9.8	More Details
CVE-2021-43466	In the thymeleaf-spring5:3.0.12 component, thymeleaf combined with specific scenarios in template injection may lead to remote code execution.	9.8	More Details
CVE-2021-31886	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions < V3.5.4), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.19), APOGEE PXC Modular (BACnet) (All versions < V3.5.4), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.19), Desigo PXC00-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC00-U (All versions >= V2.3 and < V6.30.016), Desigo PXC001-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC100-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC12-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC128-U (All versions >= V2.3 and < V6.30.016), Desigo PXC200-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC22-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC22.1-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC36.1-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC50-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC64-U (All versions >= V2.3 and < V6.30.016), Desigo PXM20-E (All versions >= V2.3 and < V6.30.016), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions < V3.5.4), TALON TC Modular (BACnet) (All versions < V3.5.4). FTP server does not properly validate the length of the “USER” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010)	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31884	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions < V3.5.4), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.19), APOGEE PXC Modular (BACnet) (All versions < V3.5.4), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.19), Capital VSTAR (All versions with enabled Ethernet options), Desigo PXC00-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC00-U (All versions >= V2.3 and < V6.30.016), Desigo PXC001-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC100-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC12-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC128-U (All versions >= V2.3 and < V6.30.016), Desigo PXC200-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC22-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC22.1-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC36.1-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC50-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC64-U (All versions >= V2.3 and < V6.30.016), Desigo PXM20-E (All versions >= V2.3 and < V6.30.016), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions < V3.5.4), TALON TC Modular (BACnet) (All versions < V3.5.4). The DHCP client application assumes that the data supplied with the “Hostname” DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014)	9.8	More Details
CVE-2021-41170	neoan3-apps/template is a neoan3 minimal template engine. Versions prior to 1.1.1 have allowed for passing in closures directly into the template engine. As a result values that are callable are executed by the template engine. The issue arises if a value has the same name as a method or function in scope and can therefore be executed either by mistake or maliciously. In theory all users of the package are affected as long as they either deal with direct user input or database values. A multi-step attack on is therefore plausible. Version 1.1.1 has addressed this vulnerability. Unfortunately only working with hardcoded values is safe in prior versions. As this likely defeats the purpose of a template engine, please upgrade.	9.8	More Details
CVE-2021-24827	The Asgaros Forum WordPress plugin before 1.15.13 does not validate and escape user input when subscribing to a topic before using it in a SQL statement, leading to an unauthenticated SQL injection issue	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24731	The Registration Forms – User profile, Content Restriction, Spam Protection, Payment Gateways, Invitation Codes WordPress plugin before 3.7.1.6 does not properly escape user data before using it in a SQL statement in the wp-json/pie/v1/login REST API endpoint, leading to an SQL injection.	9.8	More Details
CVE-2021-42665	An SQL Injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the login form inside of index.php, which can allow an attacker to bypass authentication.	9.8	More Details
CVE-2021-43572	The verify function in the Stark Bank Python ECDSA library (aka starkbank-escada or ecdsa-python) before 2.0.1 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages.	9.8	More Details
CVE-2021-20701	Buffer overflow vulnerability in the Disk Agent CLUSTERPRO X 4.3 for Windows and earlier, EXPRESSCLUSTER X 4.3 for Windows and earlier, CLUSTERPRO X 4.3 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 4.3 SingleServerSafe for Windows and earlier allows attacker to remote code execution via a network.	9.8	More Details
CVE-2021-40849	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, the account associated with a web services token is vulnerable to being exploited and logged into, resulting in information disclosure (at a minimum) and often escalation of privileges.	9.8	More Details
CVE-2021-39238	Certain HP Enterprise LaserJet, HP LaserJet Managed, HP Enterprise PageWide, HP PageWide Managed products may be vulnerable to potential buffer overflow.	9.8	More Details
CVE-2021-43082	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in the stats-over-http plugin of Apache Traffic Server allows an attacker to overwrite memory. This issue affects Apache Traffic Server 9.1.0.	9.8	More Details
CVE-2020-23679	Buffer overflow vulnerability in Renleilei1992 Linux_Network_Project 1.0, allows attackers to execute arbitrary code, via the password field.	9.8	More Details
CVE-2020-24000	SQL Injection vulnerability in eyoucms cms v1.4.7, allows attackers to execute arbitrary code and disclose sensitive information, via the tid parameter to index.php.	9.8	More Details
CVE-2020-24743	An issue was found in /showReports.do Zoho ManageEngine Applications Manager up to 14550, allows attackers to gain escalated privileges via the resourceid parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-18261	An arbitrary file upload vulnerability in the image upload function of ED01-CMS v1.0 allows attackers to execute arbitrary commands.	9.8	More Details
CVE-2020-18262	ED01-CMS v1.0 was discovered to contain a SQL injection in the component cposts.php via the cid parameter.	9.8	More Details
CVE-2020-5955	An issue was discovered in Int15MicrocodeSmm in Insyde InsydeH2O before 2021-10-14 on Intel client chipsets. A caller may be able to escalate privileges.	9.8	More Details
CVE-2021-43140	SQL Injection vulnerability exists in Sourcecodester. Simple Subscription Website 1.0. via the login.	9.8	More Details
CVE-2021-41492	Multiple SQL Injection vulnerabilities exist in Sourcecodester Simple Cashiering System (POS) 1.0 via the (1) Product Code in the pos page in cashiering. (2) id parameter in manage_products and the (3) t paramater in actions.php.	9.8	More Details
CVE-2021-42772	Broadcom Emulex HBA Manager/One Command Manager versions before 11.4.425.0 and 12.8.542.31, if not installed in Strictly Local Management mode, have a buffer overflow vulnerability in the remote GetDumpFile command that could allow a user to attempt various attacks. In non-secure mode, the user is unauthenticated	9.8	More Details
CVE-2020-25367	A command injection vulnerability was discovered in the HNAP1 protocol in D-Link DIR-823G devices with firmware V1.0.2B05. An attacker is able to execute arbitrary web scripts via shell metacharacters in the Captcha field to Login.	9.8	More Details
CVE-2021-41036	In versions prior to 1.1 of the Eclipse Paho MQTT C Client, the client does not check rem_len size in readpacket.	9.8	More Details
CVE-2020-25368	A command injection vulnerability was discovered in the HNAP1 protocol in D-Link DIR-823G devices with firmware V1.0.2B05. An attacker is able to execute arbitrary web scripts via shell metacharacters in the PrivateLogin field to Login.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40119	A vulnerability in the key-based SSH authentication mechanism of Cisco Policy Suite could allow an unauthenticated, remote attacker to log in to an affected system as the root user. This vulnerability is due to the re-use of static SSH keys across installations. An attacker could exploit this vulnerability by extracting a key from a system under their control. A successful exploit could allow the attacker to log in to an affected system as the root user.	9.8	More Details
CVE-2021-20704	Buffer overflow vulnerability in the compatible API with previous versions CLUSTERPRO X 4.3 for Windows and earlier, EXPRESSCLUSTER X 4.3 for Windows and earlier, CLUSTERPRO X 4.3 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 4.3 SingleServerSafe for Windows and earlier allows attacker to remote code execution via a network.	9.8	More Details
CVE-2021-20703	Buffer overflow vulnerability in the Transaction Server CLUSTERPRO X 4.3 for Windows and earlier, EXPRESSCLUSTER X 4.3 for Windows and earlier, CLUSTERPRO X 4.3 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 4.3 SingleServerSafe for Windows and earlier allows attacker to remote code execution via a network.	9.8	More Details
CVE-2021-20702	Buffer overflow vulnerability in the Transaction Server CLUSTERPRO X 4.3 for Windows and earlier, EXPRESSCLUSTER X 4.3 for Windows and earlier, CLUSTERPRO X 4.3 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 4.3 SingleServerSafe for Windows and earlier allows attacker to remote code execution via a network.	9.8	More Details
CVE-2021-21690	Agent processes are able to completely bypass file path filtering by wrapping the file operation in an agent file path in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	9.8	More Details
CVE-2021-21691	Creating symbolic links is possible without the 'symlink' agent-to-controller access control permission in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	9.8	More Details
CVE-2021-21692	FilePath#renameTo and FilePath#moveAllChildrenTo in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier only check 'read' agent-to-controller access permission on the source path, instead of 'delete'.	9.8	More Details
CVE-2021-21693	When creating temporary files, agent-to-controller access to create those files is only checked after they've been created in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	9.8	More Details
CVE-2021-21694	FilePath#toURI, FilePath#hasSymlink, FilePath#absolutize, FilePath#isDescendant, and FilePath#get*DiskSpace do not check any permissions in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21696	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not limit agent read/write access to the libs/ directory inside build directories when using the FilePath APIs, allowing attackers in control of agent processes to replace the code of a trusted library with a modified variant. This results in unsandboxed code execution in the Jenkins controller process.	9.8	More Details
CVE-2021-43130	An SQL Injection vulnerability exists in Sourcecodester Customer Relationship Management System (CRM) 1.0 via the username parameter in customer/login.php.	9.8	More Details
CVE-2020-20982	Cross Site Scripting (XSS) vulnerability in shadoweb wdja v1.5.1, allows attackers to execute arbitrary code and gain escalated privileges, via the backurl parameter to /php/passport/index.php.	9.6	More Details
CVE-2021-43400	An issue was discovered in gatt-database.c in BlueZ 5.61. A use-after-free can occur when a client disconnects during D-Bus processing of a WriteValue call.	9.1	More Details
CVE-2019-16240	A Buffer Overflow and Information Disclosure issue exists in HP OfficeJet Pro Printers before 001.1937C, and HP PageWide Managed Printers and HP PageWide Pro Printers before 001.1937D exists; A maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device.	9.1	More Details
CVE-2021-21697	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier allows any agent to read and write the contents of any build directory stored in Jenkins with very few restrictions.	9.1	More Details
CVE-2020-25366	An issue in the component /cgi-bin/upload_firmware.cgi of D-Link DIR-823G REVA1 1.02B05 allows attackers to cause a denial of service (DoS) via unspecified vectors.	9.1	More Details
CVE-2021-21685	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not check agent-to-controller access to create parent directories in FilePath#mkdirs.	9.1	More Details
CVE-2021-21687	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not check agent-to-controller access to create symbolic links when unarchiving a symbolic link in FilePath#untar.	9.1	More Details
CVE-2021-21689	FilePath#unzip and FilePath#untar were not subject to any agent-to-controller access control in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24693	The Simple Download Monitor WordPress plugin before 3.9.5 does not escape the "File Thumbnail" post meta before outputting it in some pages, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks. Given the that XSS is triggered even when the Download is in a review state, contributor could make JavaScript code execute in a context of a reviewer such as admin and make them create a rogue admin account, or install a malicious plugin	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-21695	FilePath#listFiles lists files outside directories that agents are allowed to access when following symbolic links in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	8.8	More Details
CVE-2021-26786	An issue was discoverered in in customercentric-selling-poland PlayTube, allows authenticated attackers to execute arbitrary code via the purchace code to the config.php.	8.8	More Details
CVE-2021-24626	The Chameleon CSS WordPress plugin through 1.2 does not have any CSRF and capability checks in all its AJAX calls, allowing any authenticated user, such as subscriber to call them and perform unauthorised actions. One of AJAX call, remove_css, also does not sanitise or escape the css_id POST parameter before using it in a SQL statement, leading to a SQL Injection	8.8	More Details
CVE-2021-41208	TensorFlow is an open source platform for machine learning. In affected versions the code for boosted trees in TensorFlow is still missing validation. As a result, attackers can trigger denial of service (via dereferencing `nullptr`s or via `CHECK`-failures) as well as abuse undefined behavior (binding references to `nullptr`s). An attacker can also read and write from heap buffers, depending on the API that gets used and the arguments that are passed to the call. Given that the boosted trees implementation in TensorFlow is unmaintained, it is recommend to no longer use these APIs. We will deprecate TensorFlow's boosted trees APIs in subsequent releases. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24575	The School Management System – WPSchoolPress WordPress plugin before 2.1.10 does not properly sanitize or use prepared statements before using POST variable in SQL queries, leading to SQL injection in multiple actions available to various authenticated users, from simple subscribers/students to teachers and above.	8.8	More Details
CVE-2021-24631	The Unlimited PopUps WordPress plugin through 4.5.3 does not sanitise or escape the did GET parameter before using it in a SQL statement, available to users as low as editor, leading to an authenticated SQL Injection	8.8	More Details
CVE-2021-24669	The MAZ Loader – Preloader Builder for WordPress plugin before 1.3.3 does not validate or escape the loader_id parameter of the mzldr shortcode, which allows users with a role as low as Contributor to perform SQL injection.	8.8	More Details
CVE-2021-43406	An issue was discovered in FusionPBX before 4.5.30. The fax_post_size may have risky characters (it is not constrained to preset values).	8.8	More Details
CVE-2020-28419	During installation with certain driver software or application packages an arbitrary code execution could occur.	8.8	More Details
CVE-2021-43413	An issue was discovered in GNU Hurd before 0.9 20210404-9. A single pager port is shared among everyone who mmaps a file, allowing anyone to modify any files that they can read. This can be trivially exploited to get full root access.	8.8	More Details
CVE-2021-31599	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. A reports (.prpt) file allows the inclusion of BeanShell scripts to ease the production of complex reports. An authenticated user can run arbitrary code.	8.8	More Details
CVE-2021-43405	An issue was discovered in FusionPBX before 4.5.30. The fax_extension may have risky characters (it is not constrained to be numeric).	8.8	More Details
CVE-2021-42072	An issue was discovered in Barrier before 2.4.0. The barriers component (aka the server-side implementation of Barrier) does not sufficiently verify the identify of connecting clients. Clients can thus exploit weaknesses in the provided protocol to cause denial-of-service or stage further attacks that could lead to information leaks or integrity corruption.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43404	An issue was discovered in FusionPBX before 4.5.30. The FAX file name may have risky characters.	8.8	More Details
CVE-2021-38501	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. 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 < 93, Thunderbird < 91.2, and Firefox ESR < 91.2.	8.8	More Details
CVE-2021-38500	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. 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 Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93.	8.8	More Details
CVE-2021-38499	Mozilla developers reported memory safety bugs present in Firefox 92. 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 < 93.	8.8	More Details
CVE-2021-38418	Delta Electronics DIALink versions 1.2.4.0 and prior runs by default on HTTP, which may allow an attacker to be positioned between the traffic and perform a machine-in-the-middle attack to access information without authorization.	8.8	More Details
CVE-2021-42666	A SQL Injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the id parameter to quiz_question.php, which could let a malicious user extract sensitive data from the web server and in some cases use this vulnerability in order to get a remote code execution on the remote web server.	8.8	More Details
CVE-2021-38496	During operations on MessageTasks, a task may have been removed while it was still scheduled, resulting in memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93.	8.8	More Details
CVE-2021-38495	Mozilla developers reported memory safety bugs present in Thunderbird 78.13.0. 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 Thunderbird < 91.1 and Firefox ESR < 91.1.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38494	Mozilla developers reported memory safety bugs present in Firefox 91. 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 < 92.	8.8	More Details
CVE-2021-38493	Mozilla developers reported memory safety bugs present in Firefox 91 and Firefox ESR 78.13. 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 ESR < 78.14, Thunderbird < 78.14, and Firefox < 92.	8.8	More Details
CVE-2021-24829	The Visitor Traffic Real Time Statistics WordPress plugin before 3.9 does not validate and escape user input passed to the today_traffic_index AJAX action (available to any authenticated users) before using it in a SQL statement, leading to an SQL injection issue	8.8	More Details
CVE-2021-43339	In Ericsson Network Location before 2021-07-31, it is possible for an authenticated attacker to inject commands via file_name in the export functionality. For example, a new admin user could be created.	8.8	More Details
CVE-2021-24835	The WCFM – Frontend Manager for WooCommerce along with Bookings Subscription Listings Compatible WordPress plugin before 6.5.12, when used in combination with another WCFM - WooCommerce Multivendor plugin such as WCFM - WooCommerce Multivendor Marketplace, does not escape the withdrawal_vendor parameter before using it in a SQL statement, allowing low privilege users such as Subscribers to perform SQL injection attacks	8.8	More Details
CVE-2020-23572	BEESCMS v4.0 was discovered to contain an arbitrary file upload vulnerability via the component /admin/upload.php. This vulnerability allows attackers to execute arbitrary code via a crafted image file.	8.8	More Details
CVE-2021-42372	A shell command injection in the HW Events SNMP community in XoruX LPAR2RRD and STOR2RRD before 7.30 allows authenticated remote attackers to execute arbitrary shell commands as the user running the service.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31887	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions < V3.5.4), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.19), APOGEE PXC Modular (BACnet) (All versions < V3.5.4), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.19), Desigo PXC00-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC00-U (All versions >= V2.3 and < V6.30.016), Desigo PXC001-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC100-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC12-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC128-U (All versions >= V2.3 and < V6.30.016), Desigo PXC200-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC22-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC22.1-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC36.1-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC50-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC64-U (All versions >= V2.3 and < V6.30.016), Desigo PXM20-E (All versions >= V2.3 and < V6.30.016), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions < V3.5.4), TALON TC Modular (BACnet) (All versions < V3.5.4). FTP server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31888	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions < V3.5.4), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.19), APOGEE PXC Modular (BACnet) (All versions < V3.5.4), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.19), Desigo PXC00-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC00-U (All versions >= V2.3 and < V6.30.016), Desigo PXC001-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC100-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC12-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC128-U (All versions >= V2.3 and < V6.30.016), Desigo PXC200-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC22-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC22.1-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC36.1-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC50-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC64-U (All versions >= V2.3 and < V6.30.016), Desigo PXM20-E (All versions >= V2.3 and < V6.30.016), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions < V3.5.4), TALON TC Modular (BACnet) (All versions < V3.5.4). FTP server does not properly validate the length of the “MKD/XMKD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018)	8.8	More Details
CVE-2021-24630	The Schreikasten WordPress plugin through 0.14.18 does not sanitise or escape the id GET parameter before using it in SQL statements in the comments dashboard from various actions, leading to authenticated SQL Injections which can be exploited by users as low as author	8.8	More Details
CVE-2021-41134	nbdime provides tools for diffing and merging of Jupyter Notebooks. In affected versions a stored cross-site scripting (XSS) issue exists within the Jupyter-owned nbdime project. It appears that when reading the file name and path from disk, the extension does not sanitize the string it constructs before returning it to be displayed. The diffNotebookCheckpoint function within nbdime causes this issue. When attempting to display the name of the local notebook (diffNotebookCheckpoint), nbdime appears to simply append .ipynb to the name of the input file. The NbdimeWidget is then created, and the base string is passed through to the request API function. From there, the frontend simply renders the HTML tag and anything along with it. Users are advised to patch to the most recent version of the affected product.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39906	Improper validation of ipynb files in GitLab CE/EE version 13.5 and above allows an attacker to execute arbitrary JavaScript code on the victim's behalf.	8.7	More Details
CVE-2021-42073	An issue was discovered in Barrier before 2.4.0. An attacker can enter an active session state with the barriers component (aka the server-side implementation of Barrier) simply by supplying a client label that identifies a valid client configuration. This label is "Unnamed" by default but could instead be guessed from hostnames or other publicly available information. In the active session state, an attacker can capture input device events from the server, and also modify the clipboard content on the server.	8.2	More Details
CVE-2021-31346	A vulnerability has been identified in Capital Embedded AR Classic 431-422 (All versions), Capital Embedded AR Classic R20-11 (All versions < V2303), PLUSCONTROL 1st Gen (All versions), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions < V1.0.0.0). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007)	8.2	More Details
CVE-2020-23109	Buffer overflow vulnerability in function convert_colorspace in heif_colorconversion.cc in libheif v1.6.2, allows attackers to cause a denial of service and disclose sensitive information, via a crafted HEIF file.	8.1	More Details
CVE-2021-34739	A vulnerability in the web-based management interface of multiple Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to replay valid user session credentials and gain unauthorized access to the web-based management interface of an affected device. This vulnerability is due to insufficient expiration of session credentials. An attacker could exploit this vulnerability by conducting a man-in-the-middle attack against an affected device to intercept valid session credentials and then replaying the intercepted credentials toward the same device at a later time. A successful exploit could allow the attacker to access the web-based management interface with administrator privileges.	8.1	More Details
CVE-2021-21686	File path filters in the agent-to-controller security subsystem of Jenkins 2.318 and earlier, LTS 2.303.2 and earlier do not canonicalize paths, allowing operations to follow symbolic links to outside allowed directories.	8.1	More Details
CVE-2021-38161	Improper Authentication vulnerability in TLS origin verification of Apache Traffic Server allows for man in the middle attacks. This issue affects Apache Traffic Server 8.0.0 to 8.0.8.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29993	Firefox for Android allowed navigations through the `intent://` protocol, which could be used to cause crashes and UI spoofs. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 92.	8.1	More Details
CVE-2021-29991	Firefox incorrectly accepted a newline in a HTTP/3 header, interpretting it as two separate headers. This allowed for a header splitting attack against servers using HTTP/3. This vulnerability affects Firefox < 91.0.1 and Thunderbird < 91.0.1.	8.1	More Details
CVE-2021-24647	The Registration Forms – User profile, Content Restriction, Spam Protection, Payment Gateways, Invitation Codes WordPress plugin before 3.1.7.6 has a flaw in the social login implementation, allowing unauthenticated attacker to login as any user on the site by only knowing their user ID or username	8.1	More Details
CVE-2021-25502	A vulnerability of storing sensitive information insecurely in Property Settings prior to SMR Nov-2021 Release 1 allows attackers to read ESN value without priviledge.	7.9	More Details
CVE-2019-18912	A potential security vulnerability has been identified for certain HP printers and MFPs with Troy solutions. For affected printers with FutureSmart Firmware bundle version 4.9 or 4.9.0.1 the potential vulnerability may cause instability in the solution.	7.8	More Details
CVE-2021-42543	The affected application uses specific functions that could be abused through a crafted project file, which could lead to code execution, system reboot, and system shutdown.	7.8	More Details
CVE-2021-42624	A local buffer overflow vulnerability exists in the latest version of Miniftpd in ftpproto.c through the tmp variable, where a crafted payload can be sent to the affected function.	7.8	More Details
CVE-2021-34597	Improper Input Validation vulnerability in PC Worx Automation Suite of Phoenix Contact up to version 1.88 could allow an attacker with a manipulated project file to unpack arbitrary files outside of the selected project directory.	7.8	More Details
CVE-2019-18916	A potential security vulnerability has been identified for HP LaserJet Solution Software (for certain HP LaserJet Printers) which may lead to unauthorized elevation of privilege on the client.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37207	A vulnerability has been identified in SENTRON powermanager V3 (All versions). The affected application assigns improper access rights to a specific folder containing configuration files. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.	7.8	More Details
CVE-2021-3927	vim is vulnerable to Heap-based Buffer Overflow	7.8	More Details
CVE-2021-41220	TensorFlow is an open source platform for machine learning. In affected versions the async implementation of `CollectiveReduceV2` suffers from a memory leak and a use after free. This occurs due to the asynchronous computation and the fact that objects that have been `std::move()`d from are still accessed. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, as this version is the only one that is also affected.	7.8	More Details
CVE-2021-38420	Delta Electronics DIALink versions 1.2.4.0 and prior default permissions give extensive permissions to low-privileged user accounts, which may allow an attacker to modify the installation directory and upload malicious files.	7.8	More Details
CVE-2021-38416	Delta Electronics DIALink versions 1.2.4.0 and prior insecurely loads libraries, which may allow an attacker to use DLL hijacking and takeover the system where the software is installed.	7.8	More Details
CVE-2021-42057	Obsidian Dataview through 0.4.12-hotfix1 allows eval injection. The evalInContext function in executes user input, which allows an attacker to craft malicious Markdown files that will execute arbitrary code once opened. NOTE: 0.4.13 provides a mitigation for some use cases.	7.8	More Details
CVE-2021-3928	vim is vulnerable to Use of Uninitialized Variable	7.8	More Details
CVE-2021-38422	Delta Electronics DIALink versions 1.2.4.0 and prior stores sensitive information in cleartext, which may allow an attacker to have extensive access to the application directory and escalate privileges.	7.8	More Details
CVE-2021-42698	Project files are stored memory objects in the form of binary serialized data that can later be read and deserialized again to instantiate the original objects in memory. Malicious manipulation of these files may allow an attacker to corrupt memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43412	An issue was discovered in GNU Hurd before 0.9 20210404-9. libports accepts fake notification messages from any client on any port, which can lead to port use-after-free. This can be exploited for local privilege escalation to get full root access.	7.8	More Details
CVE-2020-23680	An issue was discovered in function StartPage in text2pdf.c in pdfcorner text2pdf 1.1, allows attackers to cause denial of service or possibly other undisclosed impacts.	7.8	More Details
CVE-2021-41221	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for the `Cudnn*` operations in TensorFlow can be tricked into accessing invalid memory, via a heap buffer overflow. This occurs because the ranks of the `input`, `input_h` and `input_c` parameters are not validated, but code assumes they have certain values. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.8	More Details
CVE-2021-41219	TensorFlow is an open source platform for machine learning. In affected versions the code for sparse matrix multiplication is vulnerable to undefined behavior via binding a reference to `nullptr`. This occurs whenever the dimensions of `a` or `b` are 0 or less. In the case on one of these is 0, an empty output tensor should be allocated (to conserve the invariant that output tensors are always allocated when the operation is successful) but nothing should be written to it (that is, we should return early from the kernel implementation). Otherwise, attempts to write to this empty tensor would result in heap OOB access. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.8	More Details
CVE-2020-23565	Irfanview v4.53 allows attackers to execute arbitrary code via a crafted JPEG 2000 file. Related to a "Data from Faulting Address controls Branch Selection starting at JPEG2000!ShowPlugInSaveOptions_W+0x0000000000032850".	7.8	More Details
CVE-2021-41203	TensorFlow is an open source platform for machine learning. In affected versions an attacker can trigger undefined behavior, integer overflows, segfaults and `CHECK`-fail crashes if they can change saved checkpoints from outside of TensorFlow. This is because the checkpoints loading infrastructure is missing validation for invalid file formats. The fixes will be included in TensorFlow 2.7.0. We will also cherrypick these commits on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41201	TensorFlow is an open source platform for machine learning. In affeced versions during execution, `EinsumHelper::ParseEquation()` is supposed to set the flags in `input_has_ellipsis` vector and `*output_has_ellipsis` boolean to indicate whether there is ellipsis in the corresponding inputs and output. However, the code only changes these flags to `true` and never assigns `false`. This results in unitialized variable access if callers assume that `EinsumHelper::ParseEquation()` always sets these flags. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.8	More Details
CVE-2021-41214	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `tf.ragged.cross` has an undefined behavior due to binding a reference to `nullptr`. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.8	More Details
CVE-2021-40848	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, exported CSV files could contain characters that a spreadsheet program could interpret as a command, leading to execution of a malicious string locally on a device, aka CSV injection.	7.8	More Details
CVE-2020-28416	HP has identified a security vulnerability with the I.R.I.S. OCR (Optical Character Recognition) software available with HP PageWide and OfficeJet printer software installations that could potentially allow unauthorized local code execution.	7.8	More Details
CVE-2020-6931	HP Print and Scan Doctor may potentially be vulnerable to local elevation of privilege.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40359	A vulnerability has been identified in OpenPCS 7 V8.2 (All versions), OpenPCS 7 V9.0 (All versions < V9.0 Upd4), OpenPCS 7 V9.1 (All versions), SIMATIC BATCH V8.2 (All versions), SIMATIC BATCH V9.0 (All versions), SIMATIC BATCH V9.1 (All versions), SIMATIC NET PC Software V14 (All versions), SIMATIC NET PC Software V15 (All versions), SIMATIC NET PC Software V16 (All versions < V16 Update 6), SIMATIC NET PC Software V17 (All versions < V17 SP1), SIMATIC PCS 7 V8.2 (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3 UC04), SIMATIC PCS 7 V9.1 (All versions < V9.1 SP1), SIMATIC Route Control V8.2 (All versions), SIMATIC Route Control V9.0 (All versions), SIMATIC Route Control V9.1 (All versions), SIMATIC WinCC V15 and earlier (All versions < V15 SP1 Update 7), SIMATIC WinCC V16 (All versions < V16 Update 5), SIMATIC WinCC V17 (All versions < V17 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 19), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). 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.	7.7	More Details
CVE-2021-22260	A stored Cross-Site Scripting vulnerability in the DataDog integration in all versions of GitLab CE/EE starting from 13.7 before 14.0.9, all versions starting from 14.1 before 14.1.4, and all versions starting from 14.2 before 14.2.2 allows an attacker to execute arbitrary JavaScript code on the victim's behalf	7.7	More Details
CVE-2021-42075	An issue was discovered in Barrier before 2.3.4. The barriers component (aka the server-side implementation of Barrier) does not correctly close file descriptors for established TCP connections. An unauthenticated remote attacker can thus cause file descriptor exhaustion in the server process, leading to denial of service.	7.5	More Details
CVE-2021-41771	ImportedSymbols in debug/macho (for Open or OpenFat) in Go before 1.16.10 and 1.17.x before 1.17.3 Accesses a Memory Location After the End of a Buffer, aka an out-of-bounds slice situation.	7.5	More Details
CVE-2021-39182	EnroCrypt is a Python module for encryption and hashing. Prior to version 1.1.4, EnroCrypt used the MD5 hashing algorithm in the hashing file. Beginners who are unfamiliar with hashes can face problems as MD5 is considered an insecure hashing algorithm. The vulnerability is patched in v1.1.4 of the product. As a workaround, users can remove the `MD5` hashing function from the file `hashing.py`.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42074	An issue was discovered in Barrier before 2.3.4. An unauthenticated attacker can cause a segmentation fault in the barriers component (aka the server-side implementation of Barrier) by quickly opening and closing TCP connections while sending a Hello message for each TCP session.	7.5	More Details
CVE-2021-41228	TensorFlow is an open source platform for machine learning. In affected versions TensorFlow's `saved_model_cli` tool is vulnerable to a code injection as it calls `eval` on user supplied strings. This can be used by attackers to run arbitrary code on the plaform where the CLI tool runs. However, given that the tool is always run manually, the impact of this is not severe. We have patched this by adding a `safe` flag which defaults to `True` and an explicit warning for users. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.5	More Details
CVE-2021-31890	A vulnerability has been identified in Capital Embedded AR Classic 431-422 (All versions), Capital Embedded AR Classic R20-11 (All versions < V2303), PLUSCONTROL 1st Gen (All versions), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions < V1.0.0.0). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017)	7.5	More Details
CVE-2021-31889	A vulnerability has been identified in Capital Embedded AR Classic 431-422 (All versions), Capital Embedded AR Classic R20-11 (All versions < V2303), PLUSCONTROL 1st Gen (All versions), SIMOTICS CONNECT 400 (All versions < V0.5.0.0). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015)	7.5	More Details
CVE-2021-41772	Go before 1.16.10 and 1.17.x before 1.17.3 allows an archive/zip Reader.Open panic via a crafted ZIP archive containing an invalid name or an empty filename field.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31885	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions < V3.5.4), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.19), APOGEE PXC Modular (BACnet) (All versions < V3.5.4), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.19), Desigo PXC00-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC00-U (All versions >= V2.3 and < V6.30.016), Desigo PXC001-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC100-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC12-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC128-U (All versions >= V2.3 and < V6.30.016), Desigo PXC200-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC22-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC22.1-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC36.1-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC50-E.D (All versions >= V2.3 and < V6.30.016), Desigo PXC64-U (All versions >= V2.3 and < V6.30.016), Desigo PXM20-E (All versions >= V2.3 and < V6.30.016), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), PLUSCONTROL 1st Gen (All versions), TALON TC Compact (BACnet) (All versions < V3.5.4), TALON TC Modular (BACnet) (All versions < V3.5.4). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009)	7.5	More Details
CVE-2021-37471	Cradlepoint IBR900-600 devices running versions < 7.21.10 are vulnerable to a restricted shell escape sequence that provides an attacker the capability to simultaneously deny availability to the device's NetCloud Manager console, local console and SSH command-line.	7.5	More Details
CVE-2021-42076	An issue was discovered in Barrier before 2.3.4. An attacker can cause memory exhaustion in the barriers component (aka the server-side implementation of Barrier) and barrierc by sending long TCP messages.	7.5	More Details
CVE-2021-42359	WP DSGVO Tools (GDPR) <= 3.1.23 had an AJAX action, ‘admin-dismiss-unsubscribe‘, which lacked a capability check and a nonce check and was available to unauthenticated users, and did not check the post type when deleting unsubscription requests. As such, it was possible for an attacker to permanently delete an arbitrary post or page on the site by sending an AJAX request with the “action” parameter set to “admin-dismiss-unsubscribe” and the “id” parameter set to the post to be deleted. Sending such a request would move the post to the trash, and repeating the request would permanently delete the post in question.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31345	A vulnerability has been identified in Capital Embedded AR Classic 431-422 (All versions), Capital Embedded AR Classic R20-11 (All versions < V2303), PLUSCONTROL 1st Gen (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006)	7.5	More Details
CVE-2021-43411	An issue was discovered in GNU Hurd before 0.9 20210404-9. When trying to exec a setuid executable, there's a window of time when the process already has the new privileges, but still refers to the old task and is accessible through the old process port. This can be exploited to get full root access.	7.5	More Details
CVE-2021-3924	grav is vulnerable to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7.5	More Details
CVE-2021-42671	An incorrect access control vulnerability exists in Sourcecodester Engineers Online Portal in PHP in nia_munoz_monitoring_system/admin/uploads. An attacker can leverage this vulnerability in order to bypass access controls and access all the files uploaded to the web server without the need of authentication or authorization.	7.5	More Details
CVE-2021-24695	The Simple Download Monitor WordPress plugin before 3.9.6 saves logs in a predictable location, and does not have any authentication or authorisation in place to prevent unauthenticated users to download and read the logs containing Sensitive Information such as IP Addresses and Usernames	7.5	More Details
CVE-2021-42370	A password mismanagement situation exists in XoruX LPAR2RRD and STOR2RRD before 7.30 because cleartext information is present in HTML password input fields in the device properties. (Viewing the passwords requires configuring a web browser to display HTML password input fields.)	7.5	More Details
CVE-2021-43396	In iconvdata/iso-2022-jp-3.c in the GNU C Library (aka glibc) 2.34, remote attackers can force iconv() to emit a spurious '\0' character via crafted ISO-2022-JP-3 data that is accompanied by an internal state reset. This may affect data integrity in certain iconv() use cases. NOTE: the vendor states "the bug cannot be invoked through user input and requires iconv to be invoked with a NULL inbuf, which ought to require a separate application bug to do so unintentionally. Hence there's no security impact to the bug.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28022	Blind SQL injection in the login form in ServiceTonic Helpdesk software < 9.0.35937 allows attacker to exfiltrate information via specially crafted HQL-compatible time-based SQL queries.	7.5	More Details
CVE-2021-20707	Improper input validation vulnerability in the Transaction Server CLUSTERPRO X 4.3 for Windows and earlier, EXPRESSCLUSTER X 4.3 for Windows and earlier, CLUSTERPRO X 4.3 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 4.3 SingleServerSafe for Windows and earlier allows attacker to read files upload via network..	7.5	More Details
CVE-2020-18263	PHP-CMS v1.0 was discovered to contain a SQL injection vulnerability in the component search.php via the search parameter. This vulnerability allows attackers to access sensitive database information.	7.5	More Details
CVE-2021-37147	Improper input validation vulnerability in header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 8.1.2 and 9.0.0 to 9.1.0.	7.5	More Details
CVE-2021-37148	Improper input validation vulnerability in header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 8.1.2 and 9.0.0 to 9.0.1.	7.5	More Details
CVE-2021-20705	Improper input validation vulnerability in the WebManager CLUSTERPRO X 4.3 for Windows and earlier, EXPRESSCLUSTER X 4.3 for Windows and earlier, CLUSTERPRO X 4.3 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 4.3 SingleServerSafe for Windows and earlier allows attacker to remote file upload via network.	7.5	More Details
CVE-2021-37149	Improper Input Validation vulnerability in header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 8.1.2 and 9.0.0 to 9.1.0.	7.5	More Details
CVE-2021-43173	In NLnet Labs Routinator prior to 0.10.2, a validation run can be delayed significantly by an RRDP repository by not answering but slowly drip-feeding bytes to keep the connection alive. This can be used to effectively stall validation. While Routinator has a configurable time-out value for RRDP connections, this time-out was only applied to individual read or write operations rather than the complete request. Thus, if an RRDP repository sends a little bit of data before that time-out expired, it can continuously extend the time it takes for the request to finish. Since validation will only continue once the update of an RRDP repository has concluded, this delay will cause validation to stall, leading to Routinator continuing to serve the old data set or, if in the initial validation run directly after starting, never serve any data at all.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43196	In JetBrains TeamCity before 2021.1, information disclosure via the Docker Registry connection dialog is possible.	7.5	More Details
CVE-2021-43172	NLnet Labs Routinator prior to 0.10.2 happily processes a chain of RRDP repositories of infinite length causing it to never finish a validation run. In RPKI, a CA can choose the RRDP repository it wishes to publish its data in. By continuously generating a new child CA that only consists of another CA using a different RRDP repository, a malicious CA can create a chain of CAs of de-facto infinite length. Routinator prior to version 0.10.2 did not contain a limit on the length of such a chain and will therefore continue to process this chain forever. As a result, the validation run will never finish, leading to Routinator continuing to serve the old data set or, if in the initial validation run directly after starting, never serve any data at all.	7.5	More Details
CVE-2021-43174	NLnet Labs Routinator versions 0.9.0 up to and including 0.10.1, support the gzip transfer encoding when querying RRDP repositories. This encoding can be used by an RRDP repository to cause an out-of-memory crash in these versions of Routinator. RRDP uses XML which allows arbitrary amounts of white space in the encoded data. The gzip scheme compresses such white space extremely well, leading to very small compressed files that become huge when being decompressed for further processing, big enough that Routinator runs out of memory when parsing input data waiting for the next XML element.	7.5	More Details
CVE-2021-43203	In JetBrains Ktor before 1.6.4, nonce verification during the OAuth2 authentication process is implemented improperly.	7.5	More Details
CVE-2021-43182	In JetBrains Hub before 2021.1.13415, a DoS via user information is possible.	7.5	More Details
CVE-2021-43180	In JetBrains Hub before 2021.1.13690, information disclosure via avatar metadata is possible.	7.5	More Details
CVE-2021-35053	Possible system denial of service in case of arbitrary changing Firefox browser parameters. An attacker could change specific Firefox browser parameters file in a certain way and then reboot the system to make the system unbootable.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33800	In Druid 1.2.3, visiting the path with parameter in a certain function can lead to directory traversal.	7.5	More Details
CVE-2021-20706	Improper input validation vulnerability in the WebManager CLUSTERPRO X 4.3 for Windows and earlier, EXPRESSCLUSTER X 4.3 for Windows and earlier, CLUSTERPRO X 4.3 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 4.3 SingleServerSafe for Windows and earlier allows attacker to remote file upload via network.	7.5	More Details
CVE-2021-34741	A vulnerability in the email scanning algorithm of Cisco AsyncOS software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to perform a denial of service (DoS) attack against an affected device. This vulnerability is due to insufficient input validation of incoming emails. An attacker could exploit this vulnerability by sending a crafted email through Cisco ESA. A successful exploit could allow the attacker to exhaust all the available CPU resources on an affected device for an extended period of time, preventing other emails from being processed and resulting in a DoS condition.	7.5	More Details
CVE-2021-41585	Improper Input Validation vulnerability in accepting socket connections in Apache Traffic Server allows an attacker to make the server stop accepting new connections. This issue affects Apache Traffic Server 5.0.0 to 9.1.0.	7.5	More Details
CVE-2021-21698	Jenkins Subversion Plugin 2.15.0 and earlier does not restrict the name of a file when looking up a subversion key file on the controller from an agent.	7.5	More Details
CVE-2021-21688	The agent-to-controller security check FilePath#reading(FileVisitor) in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not reject any operations, allowing users to have unrestricted read access using certain operations (creating archives, FilePath#copyRecursiveTo).	7.5	More Details
CVE-2021-42021	A vulnerability has been identified in Siveillance Video DLNA Server (2019 R1), Siveillance Video DLNA Server (2019 R2), Siveillance Video DLNA Server (2019 R3), Siveillance Video DLNA Server (2020 R1), Siveillance Video DLNA Server (2020 R2), Siveillance Video DLNA Server (2020 R3), Siveillance Video DLNA Server (2021 R1). The affected application contains a path traversal vulnerability that could allow to read arbitrary files on the server that are outside the application's web document directory. An unauthenticated remote attacker could exploit this issue to access sensitive information for subsequent attacks.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41312	Affected versions of Atlassian Jira Server and Data Center allow a remote attacker who has had their access revoked from Jira Service Management to enable and disable Issue Collectors on Jira Service Management projects via an Improper Authentication vulnerability in the /secure/ViewCollectors endpoint. The affected versions are before version 8.19.1.	7.5	More Details
CVE-2021-43114	FORT Validator versions prior to 1.5.2 will crash if an RPKI CA publishes an X.509 EE certificate. This will lead to RTR clients such as BGP routers to lose access to the RPKI VRP data set, effectively disabling Route Origin Validation.	7.5	More Details
CVE-2021-38498	During process shutdown, a document could have caused a use-after-free of a languages service object, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2.	7.5	More Details
CVE-2021-40366	A vulnerability has been identified in Climatix POL909 (AWB module) (All versions < V11.42), Climatix POL909 (AWM module) (All versions < V11.34). The web server of affected devices transmits data without TLS encryption. This could allow an unauthenticated remote attacker in a man-in-the-middle position to read sensitive data, such as administrator credentials, or modify data in transit.	7.4	More Details
CVE-2021-3774	Meross Smart Wi-Fi 2 Way Wall Switch (MSS550X), on its 3.1.3 version and before, creates an open Wi-Fi Access Point without the required security measures in its initial setup. This could allow a remote attacker to obtain the Wi-Fi SSID as well as the password configured by the user from Meross app via Http/JSON plain request.	7.4	More Details
CVE-2021-43189	In JetBrains YouTrack Mobile before 2021.2, access token protection on Android is incomplete.	7.3	More Details
CVE-2021-43188	In JetBrains YouTrack Mobile before 2021.2, access token protection on iOS is incomplete.	7.3	More Details
CVE-2021-24627	The G Auto-Hyperlink WordPress plugin through 1.0.1 does not sanitise or escape an 'id' GET parameter before using it in a SQL statement, to select data to be displayed in the admin dashboard, leading to an authenticated SQL injection	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24791	The Header Footer Code Manager WordPress plugin before 1.1.14 does not validate and escape the "orderby" and "order" request parameters before using them in a SQL statement when viewing the Snippets admin dashboard, leading to SQL injections	7.2	More Details
CVE-2021-24844	The Affiliates Manager WordPress plugin before 2.8.7 does not validate the orderby parameter before using it in an SQL statement in the admin dashboard, leading to an SQL Injection issue	7.2	More Details
CVE-2021-24629	The Post Content XMLRPC WordPress plugin through 1.0 does not sanitise or escape multiple GET/POST parameters before using them in SQL statements in the admin dashboard, leading to an authenticated SQL Injections	7.2	More Details
CVE-2021-24628	The Wow Forms WordPress plugin through 3.1.3 does not sanitise or escape a 'did' GET parameter before using it in a SQL statement, when deleting a form in the admin dashboard, leading to an authenticated SQL injection	7.2	More Details
CVE-2021-43281	MyBB before 1.8.29 allows Remote Code Injection by an admin with the "Can manage settings?" permission. The Admin CP's Settings management module does not validate setting types correctly on insertion and update, making it possible to add settings of supported type "php" with PHP code, executed on Change Settings pages.	7.2	More Details
CVE-2021-24625	The SpiderCatalog WordPress plugin through 1.7.3 does not sanitise or escape the 'parent' and 'ordering' parameters from the admin dashboard before using them in a SQL statement, leading to a SQL injection when adding a category	7.2	More Details
CVE-2021-25500	A missing input validation in HDCP LDFW prior to SMR Nov-2021 Release 1 allows attackers to overwrite TZASC allowing TEE compromise.	7.2	More Details
CVE-2021-24537	The Similar Posts WordPress plugin through 3.1.5 allow high privilege users to execute arbitrary PHP code in an hardened environment (ie with DISALLOW_FILE_EDIT, DISALLOW_FILE_MODS and DISALLOW_UNFILTERED_HTML set to true) via the 'widget_rrm_similar_posts_condition' widget setting of the plugin.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41248	GraphiQL is the reference implementation of this monorepo, GraphQL IDE, an official project under the GraphQL Foundation. All versions of graphiql older than graphiql@1.4.7 are vulnerable to compromised HTTP schema introspection responses or schema prop values with malicious GraphQL type names, exposing a dynamic XSS attack surface that can allow code injection on operation autocomplete. In order for the attack to take place, the user must load a vulnerable schema in graphiql. There are a number of ways that can occur. By default, the schema URL is not attacker-controllable in graphiql or in its suggested implementations or examples, leaving only very complex attack vectors. If a custom implementation of graphiql's fetcher allows the schema URL to be set dynamically, such as a URL query parameter like ?endpoint= in graphql-playground, or a database provided value, then this custom graphiql implementation is vulnerable to phishing attacks, and thus much more readily available, low or no privelege level xss attacks. The URLs could look like any generic looking graphql schema URL. It should be noted that desktop clients such as Altair, Insomnia, Postwoman, do not appear to be impacted by this. This vulnerability does not impact codemirror-graphql, monaco-graphql or other dependents, as it exists in onHasCompletion.ts in graphiql. It does impact all forks of graphiql, and every released version of graphiql.	7.1	More Details
CVE-2021-41226	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `SparseBinCount` is vulnerable to a heap OOB access. This is because of missing validation between the elements of the `values` argument and the shape of the sparse output. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.1	More Details
CVE-2021-41212	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `tf.ragged.cross` can trigger a read outside of bounds of heap allocated array. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41249	GraphQL Playground is a GraphQL IDE for development of graphQL focused applications. All versions of graphql-playground-react older than graphql-playground-react@1.7.28 are vulnerable to compromised HTTP schema introspection responses or schema prop values with malicious GraphQL type names, exposing a dynamic XSS attack surface that can allow code injection on operation autocomplete. In order for the attack to take place, the user must load a malicious schema in graphql-playground. There are several ways this can occur, including by specifying the URL to a malicious schema in the endpoint query parameter. If a user clicks on a link to a GraphQL Playground installation that specifies a malicious server, arbitrary JavaScript can run in the user's browser, which can be used to exfiltrate user credentials or other harmful goals. If you are using graphql-playground-react directly in your client app, upgrade to version 1.7.28 or later.	7.1	More Details
CVE-2021-31881	A vulnerability has been identified in Capital Embedded AR Classic 431-422 (All versions), Capital Embedded AR Classic R20-11 (All versions < V2303). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008)	7.1	More Details
CVE-2021-41223	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `FusedBatchNorm` kernels is vulnerable to a heap OOB access. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.1	More Details
CVE-2021-41224	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `SparseFillEmptyRows` can be made to trigger a heap OOB access. This occurs whenever the size of `indices` does not match the size of `values`. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41211	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `QuantizeV2` can trigger a read outside of bounds of heap allocated array. This occurs whenever `axis` is a negative value less than `-1`. In this case, we are accessing data before the start of a heap buffer. The code allows `axis` to be an optional argument (`s` would contain an `error::NOT_FOUND` error code). Otherwise, it assumes that `axis` is a valid index into the dimensions of the `input` tensor. If `axis` is less than `-1` then this results in a heap OOB read. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, as this version is the only one that is also affected.	7.1	More Details
CVE-2021-41205	TensorFlow is an open source platform for machine learning. In affected versions the shape inference functions for the `QuantizeAndDequantizeV*` operations can trigger a read outside of bounds of heap allocated array. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.1	More Details
CVE-2021-31601	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. They implement a series of web services using the SOAP protocol to allow scripting interaction with the backend server. An authenticated user (regardless of privileges) can list all databases connection details and credentials.	7.1	More Details
CVE-2021-41210	TensorFlow is an open source platform for machine learning. In affected versions the shape inference functions for `SparseCountSparseOutput` can trigger a read outside of bounds of heap allocated array. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.1	More Details
CVE-2021-31883	A vulnerability has been identified in Capital Embedded AR Classic 431-422 (All versions), Capital Embedded AR Classic R20-11 (All versions < V2303). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013)	7.1	More Details
CVE-2021-20119	The password change utility for the Arris SurfBoard SB8200 can have safety measures bypassed that allow any logged-in user to change the administrator password.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41206	TensorFlow is an open source platform for machine learning. In affected versions several TensorFlow operations are missing validation for the shapes of the tensor arguments involved in the call. Depending on the API, this can result in undefined behavior and segfault or `CHECK`-fail related crashes but in some scenarios writes and reads from heap populated arrays are also possible. We have discovered these issues internally via tooling while working on improving/testing GPU op determinism. As such, we don't have reproducers and there will be multiple fixes for these issues. These fixes will be included in TensorFlow 2.7.0. We will also cherrypick these commits on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	7.0	More Details
CVE-2021-43414	An issue was discovered in GNU Hurd before 0.9 20210404-9. The use of an authentication protocol in the proc server is vulnerable to man-in-the-middle attacks, which can be exploited for local privilege escalation to get full root access.	7.0	More Details
CVE-2021-41174	Grafana is an open-source platform for monitoring and observability. In affected versions if an attacker is able to convince a victim to visit a URL referencing a vulnerable page, arbitrary JavaScript content may be executed within the context of the victim's browser. The user visiting the malicious link must be unauthenticated and the link must be for a page that contains the login button in the menu bar. The url has to be crafted to exploit AngularJS rendering and contain the interpolation binding for AngularJS expressions. AngularJS uses double curly braces for interpolation binding: {{ }} ex: {{constructor.constructor(‘alert(1)’)()}}. When the user follows the link and the page renders, the login button will contain the original link with a query parameter to force a redirect to the login page. The URL is not validated and the AngularJS rendering engine will execute the JavaScript expression contained in the URL. Users are advised to upgrade as soon as possible. If for some reason you cannot upgrade, you can use a reverse proxy or similar to block access to block the literal string {{ in the path.	6.9	More Details
CVE-2021-20135	Nessus versions 8.15.2 and earlier were found to contain a local privilege escalation vulnerability which could allow an authenticated, local administrator to run specific executables on the Nessus Agent host. Tenable has included a fix for this issue in Nessus 10.0.0. The installation files can be obtained from the Tenable Downloads Portal (https://www.tenable.com/downloads/nessus).	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36697	With an admin account, the .htaccess file in Artica Pandora FMS <=755 can be overwritten with the File Manager component. The new .htaccess file contains a Rewrite Rule with a type definition. A normal PHP file can be uploaded with this new "file type" and the code can be executed with an HTTP request.	6.7	More Details
CVE-2021-40124	A vulnerability in the Network Access Manager (NAM) module of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to escalate privileges on an affected device. This vulnerability is due to incorrect privilege assignment to scripts executed before user logon. An attacker could exploit this vulnerability by configuring a script to be executed before logon. A successful exploit could allow the attacker to execute arbitrary code with SYSTEM privileges.	6.7	More Details
CVE-2021-41227	TensorFlow is an open source platform for machine learning. In affected versions the `ImmutableConst` operation in TensorFlow can be tricked into reading arbitrary memory contents. This is because the `tstring` TensorFlow string class has a special case for memory mapped strings but the operation itself does not offer any support for this datatype. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	6.6	More Details
CVE-2021-38492	When delegating navigations to the operating system, Firefox would accept the `mk` scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 92, Thunderbird < 91.1, Thunderbird < 78.14, Firefox ESR < 78.14, and Firefox ESR < 91.1.	6.5	More Details
CVE-2021-24674	The Genie WP Favicon WordPress plugin through 0.5.2 does not have CSRF in place when updating the favicon, which could allow attackers to make a logged in admin change it via a CSRF attack	6.5	More Details
CVE-2021-29843	IBM MQ 9.1 LTS, 9.1 CD, 9.2 LTS, and 9.2CD is vulnerable to a denial of service attack caused by an issue processing message properties. IBM X-Force ID: 205203.	6.5	More Details
CVE-2021-38491	Mixed-content checks were unable to analyze opaque origins which led to some mixed content being loaded. This vulnerability affects Firefox < 92.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38497	Through use of reportValidity() and window.open(), a plain-text validation message could have been overlaid on another origin, leading to possible user confusion and spoofing attacks. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2.	6.5	More Details
CVE-2021-27836	An issue was discoverered in in function xls_getWorkSheet in xls.c in libxls 1.6.2, allows attackers to cause a denial of service, via a crafted XLS file.	6.5	More Details
CVE-2021-24721	The Loco Translate WordPress plugin before 2.5.4 mishandles data inputs which get saved to a file, which can be renamed to an extension ending in .php, resulting in authenticated "translator" users being able to inject PHP code into files ending with .php in web accessible locations.	6.5	More Details
CVE-2021-24783	The Post Expirator WordPress plugin before 2.6.0 does not have proper capability checks in place, which could allow users with a role as low as Contributor to schedule deletion of arbitrary posts.	6.5	More Details
CVE-2021-24766	The 404 to 301 – Redirect, Log and Notify 404 Errors WordPress plugin before 3.0.9 does not have CSRF check in place when cleaning the logs, which could allow attacker to make a logged in admin delete all of them via a CSRF attack	6.5	More Details
CVE-2021-39903	In all versions of GitLab CE/EE since version 13.0, a privileged user, through an API call, can change the visibility level of a group or a project to a restricted option even after the instance administrator sets that visibility option as restricted in settings.	6.5	More Details
CVE-2021-34594	TwinCAT OPC UA Server in TF6100 and TS6100 in product versions before 4.3.48.0 or with TcOpcUaServer versions below 3.2.0.194 are prone to a relative path traversal that allow administrators to create or delete any files on the system.	6.5	More Details
CVE-2021-31882	A vulnerability has been identified in Capital Embedded AR Classic 431-422 (All versions), Capital Embedded AR Classic R20-11 (All versions < V2303). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011)	6.5	More Details
CVE-2021-3916	bookstack is vulnerable to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34773	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. These actions could include modifying the device configuration and deleting (but not creating) user accounts.	6.5	More Details
CVE-2021-40120	A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker with administrative privileges to inject arbitrary commands into the underlying operating system and execute them using root-level privileges. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to a specific field in the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as a user with root-level privileges.	6.5	More Details
CVE-2021-24767	The Redirect 404 Error Page to Homepage or Custom Page with Logs WordPress plugin before 1.7.9 does not check for CSRF when deleting logs, which could allow attacker to make a logged in admin delete them via a CSRF attack	6.5	More Details
CVE-2021-24788	The Batch Cat WordPress plugin through 0.3 defines 3 custom AJAX actions, which both require authentication but are available for all roles. As a result, any authenticated user (including simple subscribers) can add/set/delete arbitrary categories to posts.	6.5	More Details
CVE-2021-42025	A vulnerability has been identified in Mendix Applications using Mendix 8 (All versions < V8.18.13), Mendix Applications using Mendix 9 (All versions < V9.6.2). Applications built with affected versions of Mendix Studio Pro do not properly control write access for certain client actions. This could allow authenticated attackers to manipulate the content of System.FileDocument objects in some cases, regardless whether they have write access to it.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22051	Applications using Spring Cloud Gateway are vulnerable to specifically crafted requests that could make an extra request on downstream services. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.5+, 2.2.x users should upgrade to 2.2.10.RELEASE or newer.	6.5	More Details
CVE-2020-21139	EC Cloud E-Commerce System v1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily add admin accounts via /admin.html?do=user&act=add.	6.5	More Details
CVE-2021-22960	The parse function in llhttp < 2.1.4 and < 6.0.6. ignores chunk extensions when parsing the body of chunked requests. This leads to HTTP Request Smuggling (HRS) under certain conditions.	6.5	More Details
CVE-2021-32481	Cloudera Hue 4.6.0 allows XSS via the type parameter.	6.1	More Details
CVE-2021-40261	Multiple Cross Site Scripting (XSS) vulnerabilities exist in SourceCodester CASAP Automated Enrollment System 1.0 via the (1) user_username and (2) category parameters in save_class.php, the (3) firstname, (4) class, and (5) status parameters in student_table.php, the (6) category and (7) class_name parameters in add_class1.php, the (8) fname, (9) mname, (10) lname, (11) address, (12) class, (13) gfname, (14) gmname, (15) glname, (16) rship, (17) status, (18) transport, and (19) route parameters in add_student.php, the (20) fname, (21) mname, (22) lname, (23) address, (24) class, (25) fgname, (26) gmname, (27) glname, (28) rship, (29) status, (30) transport, and (31) route parameters in save_stud.php,the (32) status, (33) fname, and (34) lname parameters in add_user.php, the (35) username, (36) firstname, and (37) status parameters in users.php, the (38) fname, (39) lname, and (40) status parameters in save_user.php, and the (41) activity_log, (42) aprjun, (43) class, (44) janmar, (45) Julsep,(46) octdec, (47) Students and (48) users parameters in table_name.	6.1	More Details
CVE-2019-18914	A potential security vulnerability has been identified for certain HP printers and MFPs that would allow redirection page Cross-Site Scripting in a client's browser by clicking on a third-party malicious link.	6.1	More Details
CVE-2021-29243	Cloudera Manager 5.x, 6.x, 7.1.x, 7.2.x, and 7.3.x allows XSS.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29994	Cloudera Hue 4.6.0 allows XSS.	6.1	More Details
CVE-2021-3641	Improper Link Resolution Before File Access ('Link Following') vulnerability in the EPAG component of Bitdefender Endpoint Security Tools for Windows allows a local attacker to cause a denial of service. This issue affects: Bitdefender GravityZone version 7.1.2.33 and prior versions.	6.1	More Details
CVE-2021-42078	PHP Event Calendar through 2021-11-04 allows persistent cross-site scripting (XSS), as demonstrated by the /server/ajax/events_manager.php title parameter. This can be exploited by an adversary in multiple ways, e.g., to perform actions on the page in the context of other users, or to deface the site.	6.1	More Details
CVE-2021-43324	LibreNMS through 21.10.2 allows XSS via a widget title.	6.1	More Details
CVE-2021-35489	Thruk 2.40-2 allows /thruk/#cgi-bin/extinfo.cgi?type=2&host={HOSTNAME]&service={SERVICENAME]&backend={BACKEND] Reflected XSS via the host or service parameter. An attacker could inject arbitrary JavaScript into extinfo.cgi. The malicious payload would be triggered every time an authenticated user browses the page containing it.	6.1	More Details
CVE-2021-32482	Cloudera Manager 5.x, 6.x, 7.1.x, 7.2.x, and 7.3.x allows XSS via the path parameter.	6.1	More Details
CVE-2021-40260	Multiple Cross Site Scripting (XSS) vulnerabilities exist in SourceCodester Tailor Management 1.0 via the (1) eid parameter in (a) partedit.php and (b) customeredit.php, the (2) id parameter in (a) editmeasurement.php and (b) addpayment.php, and the (3) error parameter in index.php.	6.1	More Details
CVE-2021-35488	Thruk 2.40-2 allows /thruk/#cgi-bin/status.cgi?style=combined&title={TITLE] Reflected XSS via the host or title parameter. An attacker could inject arbitrary JavaScript into status.cgi. The payload would be triggered every time an authenticated user browses the page containing it.	6.1	More Details
CVE-2021-42770	A Cross-site scripting (XSS) vulnerability was discovered in OPNsense before 21.7.4 via the LDAP attribute return in the authentication tester.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41733	Oppia 3.1.4 does not verify that certain URLs are valid before navigating to them.	6.1	More Details
CVE-2021-40115	A vulnerability in Cisco Webex Video Mesh could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2020-23126	Chamilo LMS version 1.11.10 contains an XSS vulnerability in the personal profile edition form, affecting the user him/herself and social network friends.	6.1	More Details
CVE-2021-24697	The Simple Download Monitor WordPress plugin before 3.9.5 does not escape the 1) sdm_active_tab GET parameter and 2) sdm_stats_start_date/sdm_stats_end_date POST parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2021-43197	In JetBrains TeamCity before 2021.1.2, email notifications could include unescaped HTML for XSS.	6.1	More Details
CVE-2021-43141	Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Simple Subscription Website 1.0 via the id parameter in plan_application.	6.1	More Details
CVE-2020-22222	Stivasoft (Phpjabbers) Fundraising Script v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the pjActionLoadCss function.	6.1	More Details
CVE-2020-22224	Stivasoft (Phpjabbers) Fundraising Script v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the pjActionPreview function.	6.1	More Details
CVE-2021-24798	The WP Header Images WordPress plugin before 2.0.1 does not sanitise and escape the t parameter before outputting it back in the plugin's settings page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-39420	Multiple Cross Site Scripting (XSS) vulnerabilities exist in VFront 0.99.5 via the (1) s parameter in search_all.php and the (2) msg parameter in add.attach.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-18259	ED01-CMS v1.0 was discovered to contain a reflective cross-site scripting (XSS) vulnerability in the component sposts.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the Post title or Post content fields.	6.1	More Details
CVE-2021-39413	Multiple Cross Site Scripting (XSS) vulnerabilities exits in SEO Panel v4.8.0 via the (1) to_time parameter in (a) backlinks.php, (b) analytics.php, (c) log.php, (d) overview.php, (e) pagespeed.php, (f) rank.php, (g) review.php, (h) saturationchecker.php, (i) social_media.php, and (j) reports.php; the (2) from_time parameter in (a) backlinks.php, (b) analytics.php, (c) log.php, (d) overview.php, (e) pagespeed.php, (f) rank.php, (g) review.php, (h) saturationchecker.php, (i) social_media.php, (j) webmaster-tools.php, and (k) reports.php; the (3) order_col parameter in (a) analytics.php, (b) review.php, (c) social_media.php, and (d) webmaster-tools.php; and the (4) pageno parameter in (a) alerts.php, (b) log.php, (c) keywords.php, (d) proxy.php, (e) searchengine.php, and (f) siteauditor.php.	6.1	More Details
CVE-2021-41562	A vulnerability in Snow Snow Agent for Windows allows a non-admin user to cause arbitrary deletion of files. This issue affects: Snow Snow Agent for Windows version 5.0.0 to 6.7.1 on Windows.	6.1	More Details
CVE-2021-43181	In JetBrains Hub before 2021.1.13690, stored XSS is possible.	6.1	More Details
CVE-2021-39411	Multiple Cross Site Scripting (XSS) vulnerabilities exist in PHPGurukul Hospital Management System 4.0 via the (1) searchdata parameter in (a) doctor/search.php and (b) admin/patient-search.php, and the (2) fromdate and (3) todate parameters in admin/betweendates-detailsreports.php.	6.1	More Details
CVE-2021-39416	Multiple Cross Site Scripting (XSS) vulnerabilities exists in Remote Clinic v2.0 in (1) patients/register-patient.php via the (a) Contact, (b) Email, (c) Weight, (d) Profession, (e) ref_contact, (f) address, (g) gender, (h) age, and (i) serial parameters; in (2) patients/edit-patient.php via the (a) Contact, (b) Email, (c) Weight, Profession, (d) ref_contact, (e) address, (f) serial, (g) age, and (h) gender parameters; in (3) staff/edit-my-profile.php via the (a) Title, (b) First Name, (c) Last Name, (d) Skype, and (e) Address parameters; and in (4) clinics/settings.php via the (a) portal_name, (b) guardian_short_name, (c) guardian_name, (d) opening_time, (e) closing_time, (f) access_level_5, (g) access_level_4, (h) access_level_ 3, (i) access_level_2, (j) access_level_1, (k) currency, (l) mobile_number, (m) address, (n) patient_contact, (o) patient_address, and (p) patient_email parameters.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39412	Multiple Cross Site Scripting (XSS) vulnerabilities exists in PHPGurukul Shopping v3.1 via the (1) callback parameter in (a) server_side/scripts/id_jsonp.php, (b) server_side/scripts/jsonp.php, and (c) scripts/objects_jsonp.php, the (2) value parameter in examples_support/editable_ajax.php, and the (3) PHP_SELF parameter in captcha/index.php.	6.1	More Details
CVE-2021-39895	In all versions of GitLab CE/EE since version 8.0, an attacker can set the pipeline schedules to be active in a project export so when an unsuspecting owner imports that project, pipelines are active by default on that project. Under specialized conditions, this may lead to information disclosure if the project is imported from an untrusted source.	6.0	More Details
CVE-2021-29753	IBM Business Automation Workflow 18. 19, 20, 21, and IBM Business Process Manager 8.5 and d8.6 transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval.	5.9	More Details
CVE-2021-38502	Thunderbird ignored the configuration to require STARTTLS security for an SMTP connection. A MITM could perform a downgrade attack to intercept transmitted messages, or could take control of the authenticated session to execute SMTP commands chosen by the MITM. If an unprotected authentication method was configured, the MITM could obtain the authentication credentials, too. This vulnerability affects Thunderbird < 91.2.	5.9	More Details
CVE-2021-38424	The tag interface of Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to an attacker injecting formulas into the tag data. Those formulas may then be executed when it is opened with a spreadsheet application.	5.9	More Details
CVE-2020-4152	IBM QRadar Network Security 5.4.0 and 5.5.0 transmits sensitive or security-critical data in cleartext in a communication channel that can be obtained using man in the middle techniques. IBM X-Force ID: 17467.	5.9	More Details
CVE-2020-4160	IBM QRadar Network Security 5.4.0 and 5.5.0 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 174340.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41251	@sap-cloud-sdk/core contains the core functionality of the SAP Cloud SDK as well as the SAP Business Technology Platform abstractions. This affects applications on SAP Business Technology Platform that use the SAP Cloud SDK and enabled caching of destinations. In affected versions and in some cases, when user information was missing, destinations were cached without user information, allowing other users to retrieve the same destination with its permissions. By default, destination caching is disabled. The security for caching has been increased. The changes are released in version 1.52.0. Users unable to upgrade are advised to disable destination caching (it is disabled by default).	5.9	More Details
CVE-2021-25509	A missing input validation in Samsung Flow Windows application prior to Version 4.8.5.0 allows attackers to overwrite abtraty file in the Windows known folders.	5.9	More Details
CVE-2021-41253	Zydis is an x86/x86-64 disassembler library. Users of Zydis versions v3.2.0 and older that use the string functions provided in `zycore` in order to append untrusted user data to the formatter buffer within their custom formatter hooks can run into heap buffer overflows. Older versions of Zydis failed to properly initialize the string object within the formatter buffer, forgetting to initialize a few fields, leaving their value to chance. This could then in turn cause zycore functions like `ZyanStringAppend` to make incorrect calculations for the new target size, resulting in heap memory corruption. This does not affect the regular uncustomized Zydis formatter, because Zydis internally doesn't use the string functions in zycore that act upon these fields. However, because the zycore string functions are the intended way to work with the formatter buffer for users of the library that wish to extend the formatter, we still consider this to be a vulnerability in Zydis. This bug is patched starting in version 3.2.1. As a workaround, users may refrain from using zycore string functions in their formatter hooks until updating to a patched version.	5.9	More Details
CVE-2021-42699	The affected product is vulnerable to cookie information being transmitted as cleartext over HTTP. An attacker can capture network traffic, obtain the user’s cookie and take over the account.	5.7	More Details
CVE-2021-25501	An improper access control vulnerability in SCloudBnRReceiver in SecTelephonyProvider prior to SMR Nov-2021 Release 1 allows untrusted application to call some protected providers.	5.7	More Details
CVE-2021-25507	Improper authorization vulnerability in Samsung Flow mobile application prior to 4.8.03.5 allows Samsung Flow PC application connected with user device to access part of notification data in Secure Folder without authorization.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23624	This affects the package dotty before 0.1.2. A type confusion vulnerability can lead to a bypass of CVE-2021-25912 when the user-provided keys used in the path parameter are arrays.	5.6	More Details
CVE-2021-23509	This affects the package json-ptr before 3.0.0. A type confusion vulnerability can lead to a bypass of CVE-2020-7766 when the user-provided keys used in the pointer parameter are arrays.	5.6	More Details
CVE-2021-23807	This affects the package jsonpointer before 5.0.0. A type confusion vulnerability can lead to a bypass of a previous Prototype Pollution fix when the pointer components are arrays.	5.6	More Details
CVE-2021-23820	This affects all versions of package json-pointer. A type confusion vulnerability can lead to a bypass of CVE-2020-7709 when the pointer components are arrays.	5.6	More Details
CVE-2021-42015	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.26), Mendix Applications using Mendix 8 (All versions < V8.18.12), Mendix Applications using Mendix 9 (All versions < V9.6.1). Applications built with affected versions of Mendix Studio Pro do not prevent file documents from being cached when files are opened or downloaded using a browser. This could allow a local attacker to read those documents by exploring the browser cache.	5.5	More Details
CVE-2020-10052	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.12). The affected application writes sensitive data, such as usernames and passwords in log files. A local attacker with access to the log files could use this information to launch further attacks.	5.5	More Details
CVE-2020-10053	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.12). The affected application writes sensitive data, such as database credentials in configuration files. A local attacker with access to the configuration files could use this information to launch further attacks.	5.5	More Details
CVE-2020-10054	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.12). The affected application does not properly handle the import of large configuration files. A local attacker could import a specially crafted file which could lead to a denial-of-service condition of the application service.	5.5	More Details
CVE-2021-37850	ESET was made aware of a vulnerability in its consumer and business products for macOS that enables a user logged on to the system to stop the ESET daemon, effectively disabling the protection of the ESET security product until a system reboot.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43519	Stack overflow in lua_resume of ldo.c in Lua Interpreter 5.1.0~5.4.4 allows attackers to perform a Denial of Service via a crafted script file.	5.5	More Details
CVE-2021-40364	A vulnerability has been identified in SIMATIC PCS 7 V8.2 (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3 UC04), SIMATIC PCS 7 V9.1 (All versions < V9.1 SP1), SIMATIC WinCC V15 and earlier (All versions < V15 SP1 Update 7), SIMATIC WinCC V16 (All versions < V16 Update 5), SIMATIC WinCC V17 (All versions < V17 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 19), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). The affected systems store sensitive information in log files. An attacker with access to the log files could publicly expose the information or reuse it to develop further attacks on the system.	5.5	More Details
CVE-2021-41215	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `DeserializeSparse` can trigger a null pointer dereference. This is because the shape inference function assumes that the `serialize_sparse` tensor is a tensor with positive rank (and having `3` as the last dimension). The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-43575	KNX ETS6 through 6.0.0 uses the hard-coded password ETS5Password, with a salt value of Ivan Medvedev, allowing local users to read project information, a similar issue to CVE-2021-36799. NOTE: The vendor disputes this because it is not the responsibility of the ETS to securely store cryptographic key material when it is not being exported	5.5	More Details
CVE-2020-23567	Irfanview v4.53 allows attackers to to cause a denial of service (DoS) via a crafted JPEG 2000 file. Related to "Integer Divide By Zero starting at JPEG2000!ShowPlugInSaveOptions_W+0x00000000000082ea"	5.5	More Details
CVE-2021-41218	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `AllToAll` can be made to execute a division by 0. This occurs whenever the `split_count` argument is 0. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41207	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `ParallelConcat` misses some input validation and can produce a division by 0. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-41202	TensorFlow is an open source platform for machine learning. In affected versions while calculating the size of the output within the `tf.range` kernel, there is a conditional statement of type `int64 = condition ? int64 : double`. Due to C++ implicit conversion rules, both branches of the condition will be cast to `double` and the result would be truncated before the assignment. This result in overflows. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-41217	TensorFlow is an open source platform for machine learning. In affected versions the process of building the control flow graph for a TensorFlow model is vulnerable to a null pointer exception when nodes that should be paired are not. This occurs because the code assumes that the first node in the pairing (e.g., an `Enter` node) always exists when encountering the second node (e.g., an `Exit` node). When this is not the case, `parent` is `nullptr` so dereferencing it causes a crash. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-41200	TensorFlow is an open source platform for machine learning. In affected versions if `tf.summary.create_file_writer` is called with non-scalar arguments code crashes due to a `CHECK`-fail. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-41199	TensorFlow is an open source platform for machine learning. In affected versions if `tf.image.resize` is called with a large input argument then the TensorFlow process will crash due to a `CHECK`-failure caused by an overflow. The number of elements in the output tensor is too much for the `int64_t` type and the overflow is detected via a `CHECK` statement. This aborts the process. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41198	TensorFlow is an open source platform for machine learning. In affected versions if `tf.tile` is called with a large input argument then the TensorFlow process will crash due to a `CHECK`-failure caused by an overflow. The number of elements in the output tensor is too much for the `int64_t` type and the overflow is detected via a `CHECK` statement. This aborts the process. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-41197	TensorFlow is an open source platform for machine learning. In affected versions TensorFlow allows tensor to have a large number of dimensions and each dimension can be as large as desired. However, the total number of elements in a tensor must fit within an `int64_t`. If an overflow occurs, `MultiplyWithoutOverflow` would return a negative result. In the majority of TensorFlow codebase this then results in a `CHECK`-failure. Newer constructs exist which return a `Status` instead of crashing the binary. This is similar to CVE-2021-29584. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-41196	TensorFlow is an open source platform for machine learning. In affected versions the Keras pooling layers can trigger a segfault if the size of the pool is 0 or if a dimension is negative. This is due to the TensorFlow's implementation of pooling operations where the values in the sliding window are not checked to be strictly positive. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-41195	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `tf.math.segment_*` operations results in a `CHECK`-fail related abort (and denial of service) if a segment id in `segment_ids` is large. This is similar to CVE-2021-29584 (and similar other reported vulnerabilities in TensorFlow, localized to specific APIs): the implementation (both on CPU and GPU) computes the output shape using `AddDim`. However, if the number of elements in the tensor overflows an `int64_t` value, `AddDim` results in a `CHECK` failure which provokes a `std::abort`. Instead, code should use `AddDimWithStatus`. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23566	Irfanview v4.53 was discovered to contain an infinity loop via JPEG2000!ShowPlugInSaveOptions_W+0x1ecd8.	5.5	More Details
CVE-2021-38403	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter supplier of the API maintenance, which may allow an attacker to remotely execute code.	5.5	More Details
CVE-2021-38407	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter name of the API devices, which may allow an attacker to remotely execute code.	5.5	More Details
CVE-2021-38411	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter deviceName of the API modbusWriter-Reader, which may allow an attacker to remotely execute code.	5.5	More Details
CVE-2021-38488	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter comment of the API events, which may allow an attacker to remotely execute code.	5.5	More Details
CVE-2021-38428	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter name of the API schedule, which may allow an attacker to remotely execute code.	5.5	More Details
CVE-2021-41209	TensorFlow is an open source platform for machine learning. In affected versions the implementations for convolution operators trigger a division by 0 if passed empty filter tensor arguments. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-41204	TensorFlow is an open source platform for machine learning. In affected versions during TensorFlow's Grappler optimizer phase, constant folding might attempt to deep copy a resource tensor. This results in a segfault, as these tensors are supposed to not change. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41213	TensorFlow is an open source platform for machine learning. In affected versions the code behind `tf.function` API can be made to deadlock when two `tf.function` decorated Python functions are mutually recursive. This occurs due to using a non-reentrant `Lock` Python object. Loading any model which contains mutually recursive functions is vulnerable. An attacker can cause denial of service by causing users to load such models and calling a recursive `tf.function`, although this is not a frequent scenario. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-41216	TensorFlow is an open source platform for machine learning. In affected versions the shape inference function for `Transpose` is vulnerable to a heap buffer overflow. This occurs whenever `perm` contains negative elements. The shape inference function does not validate that the indices in `perm` are all valid. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-41222	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `SplitV` can trigger a segfault is an attacker supplies negative arguments. This occurs whenever `size_splits` contains more than one value and at least one value is negative. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-43389	An issue was discovered in the Linux kernel before 5.14.15. There is an array-index-out-of-bounds flaw in the detach_capi_ctr function in drivers/isdn/capi/kcapi.c.	5.5	More Details
CVE-2021-41225	TensorFlow is an open source platform for machine learning. In affected versions TensorFlow's Grappler optimizer has a use of unitialized variable. If the `train_nodes` vector (obtained from the saved model that gets optimized) does not contain a `Dequeue` node, then `dequeue_node` is left unitialized. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	5.5	More Details
CVE-2021-40985	A stack-based buffer under-read in htmldoc before 1.9.12, allows attackers to cause a denial of service via a crafted BMP image to image_load_bmp.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40577	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Online Enrollment Management System in PHP and PayPal Free Source Code 1.0 in the Add-Users page via the Name parameter.	5.4	More Details
CVE-2021-42662	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Online Event Booking and Reservation System in PHP/MySQL via the Holiday reason parameter. An attacker can leverage this vulnerability in order to run javascript commands on the web server surfers behalf, which can lead to cookie stealing and more.	5.4	More Details
CVE-2021-42664	A Stored Cross Site Scripting (XSS) Vulneraibiilty exists in Sourcecodester Engineers Online Portal in PHP via the (1) Quiz title and (2) quiz description parameters to add_quiz.php. An attacker can leverage this vulnerability in order to run javascript commands on the web server surfers behalf, which can lead to cookie stealing and more.	5.4	More Details
CVE-2021-25978	Apostrophe CMS versions between 2.63.0 to 3.3.1 are vulnerable to Stored XSS where an editor uploads an SVG file that contains malicious JavaScript onto the Images module, which triggers XSS once viewed.	5.4	More Details
CVE-2021-24807	The Support Board WordPress plugin before 3.3.5 allows Authenticated (Agent+) users to perform Cross-Site Scripting attacks by placing a payload in the notes field, when an administrator or any authenticated user go to the chat the XSS will be automatically executed.	5.4	More Details
CVE-2020-4153	IBM QRadar Network Security 5.4.0 and 5.5.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174269.	5.4	More Details
CVE-2021-1500	A vulnerability in the web-based management interface of Cisco Webex Video Mesh could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the URL parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. Attackers may use this type of vulnerability, known as an open redirect attack, as part of a phishing attack to persuade users to unknowingly visit malicious sites.	5.4	More Details
CVE-2021-29735	IBM Security Guardium 10.5, 10.6, 11.0, 11.1, 11.2, and 11.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34784	A vulnerability in the web-based management interface of Cisco Prime Infrastructure (PI) and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	5.4	More Details
CVE-2021-36698	Pandora FMS through 755 allows XSS via a new Event Filter with a crafted name.	5.4	More Details
CVE-2021-26844	A cross-site scripting (XSS) vulnerability in Power Admin PA Server Monitor 8.2.1.1 allows remote attackers to inject arbitrary web script or HTML via Console.exe.	5.4	More Details
CVE-2021-43184	In JetBrains YouTrack before 2021.3.21051, stored XSS is possible.	5.4	More Details
CVE-2021-23784	This affects the package tempura before 0.4.0. If the input to the esc function is of type object (i.e an array) it is returned without being escaped/sanitized, leading to a potential Cross-Site Scripting vulnerability.	5.4	More Details
CVE-2021-43186	JetBrains YouTrack before 2021.3.24402 is vulnerable to stored XSS.	5.4	More Details
CVE-2021-43198	In JetBrains TeamCity before 2021.1.2, stored XSS is possible.	5.4	More Details
CVE-2021-31344	A vulnerability has been identified in Capital Embedded AR Classic 431-422 (All versions), Capital Embedded AR Classic R20-11 (All versions < V2303), PLUSCONTROL 1st Gen (All versions), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions < V1.0.0.0). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004)	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43194	In JetBrains TeamCity before 2021.1.2, user enumeration was possible.	5.3	More Details
CVE-2021-39909	Lack of email address ownership verification in the CODEOWNERS feature in all versions of GitLab EE starting from 11.3 before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 allows an attacker to bypass CODEOWNERS Merge Request approval requirement under rare circumstances	5.3	More Details
CVE-2021-39912	A potential DoS vulnerability was discovered in GitLab CE/EE starting with version 13.7. Using a malformed TIFF images was possible to trigger memory exhaustion.	5.3	More Details
CVE-2021-39907	A potential DOS vulnerability was discovered in GitLab CE/EE starting with version 13.7. The stripping of EXIF data from certain images resulted in high CPU usage.	5.3	More Details
CVE-2021-43187	In JetBrains YouTrack Mobile before 2021.2, the client-side cache on iOS could contain sensitive information.	5.3	More Details
CVE-2021-43195	In JetBrains TeamCity before 2021.1.2, some HTTP security headers were missing.	5.3	More Details
CVE-2021-43192	In JetBrains YouTrack Mobile before 2021.2, iOS URL scheme hijacking is possible.	5.3	More Details
CVE-2021-40128	A vulnerability in the account activation feature of Cisco Webex Meetings could allow an unauthenticated, remote attacker to send an account activation email with an activation link that points to an arbitrary domain. This vulnerability is due to insufficient validation of user-supplied parameters. An attacker could exploit this vulnerability by sending a crafted HTTP request to the account activation page of Cisco Webex Meetings. A successful exploit could allow the attacker to send to any recipient an account activation email that contains a tampered activation link, which could direct the user to an attacker-controlled website.	5.3	More Details
CVE-2021-43191	JetBrains YouTrack Mobile before 2021.2, is missing the security screen on Android and iOS.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43190	In JetBrains YouTrack Mobile before 2021.2, task hijacking on Android is possible.	5.3	More Details
CVE-2021-43398	Crypto++ (aka Cryptopp) 8.6.0 and earlier contains a timing leakage in MakePublicKey(). There is a clear correlation between execution time and private key length, which may cause disclosure of the length information of the private key. This might allow attackers to conduct timing attacks. NOTE: this report is disputed by the vendor and multiple third parties. The execution-time differences are intentional. A user may make a choice of a longer key as a tradeoff between strength and performance. In making this choice, the amount of information leaked to an adversary is of infinitesimal value	5.3	More Details
CVE-2021-32483	Cloudera Manager 7.2.4 has Incorrect Access Control, allowing Escalation of Privileges to view the restricted Dashboard.	5.3	More Details
CVE-2021-25508	Improper privilege management vulnerability in API Key used in SmartThings prior to 1.7.73.22 allows an attacker to abuse the API key without limitation.	5.3	More Details
CVE-2021-24840	The Squaretype WordPress theme before 3.0.4 allows unauthenticated users to manipulate the query_vars used to retrieve the posts to display in one of its REST endpoint, without any validation. As a result, private and scheduled posts could be retrieved via a crafted request.	5.3	More Details
CVE-2021-31602	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. The Security Model has different layers of Access Control. One of these layers is the applicationContext security, which is defined in the applicationContext-spring-security.xml file. The default configuration allows an unauthenticated user with no previous knowledge of the platform settings to extract pieces of information without possessing valid credentials.	5.3	More Details
CVE-2021-33209	An issue was discovered in Fimer Aurora Vision before 2.97.10. The response to a failed login attempt discloses whether the username or password is wrong, helping an attacker to enumerate usernames. This can make a brute-force attack easier.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41230	Pomerium is an open source identity-aware access proxy. In affected versions changes to the OIDC claims of a user after initial login are not reflected in policy evaluation when using `allowed_idp_claims` as part of policy. If using `allowed_idp_claims` and a user's claims are changed, Pomerium can make incorrect authorization decisions. This issue has been resolved in v0.15.6. For users unable to upgrade clear data on `databroker` service by clearing redis or restarting the in-memory databroker to force claims to be updated.	5.3	More Details
CVE-2021-40127	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition.	5.3	More Details
CVE-2021-43199	In JetBrains TeamCity before 2021.1.2, permission checks in the Create Patch functionality are insufficient.	5.3	More Details
CVE-2021-43201	In JetBrains TeamCity before 2021.1.3, a newly created project could take settings from an already deleted project.	5.3	More Details
CVE-2021-36192	An exposure of sensitive information to an unauthorized actor [CWE-200] vulnerability in FortiManager 7.0.1 and below, 6.4.6 and below, 6.2.x, 6.0.x, 5.6.0 may allow a FortiGate user to see scripts from other ADOMS.	5.2	More Details
CVE-2021-25503	Improper input validation vulnerability in HDCP prior to SMR Nov-2021 Release 1 allows attackers to arbitrary code execution.	5.0	More Details
CVE-2021-42701	An attacker could prepare a specially crafted project file that, if opened, would attempt to connect to the cloud and trigger a man in the middle (MiTM) attack. This could allow an attacker to obtain credentials and take over the user’s cloud account.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34774	A vulnerability in the web-based management interface of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to access sensitive data on an affected system. This vulnerability exists because the application does not sufficiently protect sensitive data when responding to a specific API request. An attacker could exploit the vulnerability by sending a crafted HTTP request to the affected application. A successful exploit could allow the attacker to obtain sensitive information about the users of the application, including security questions and answers. To exploit this vulnerability an attacker would need valid Administrator credentials. Cisco expects to release software updates that address this vulnerability.	4.9	More Details
CVE-2021-24710	The Print-O-Matic WordPress plugin before 2.0.3 does not escape some of its settings before outputting them in attribute, 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-2021-24594	The Translate WordPress – Google Language Translator WordPress plugin before 6.0.12 does not sanitise and escape some of its settings before outputting it in various pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-34731	A vulnerability in the web-based management interface of Cisco Prime Access Registrar could allow an authenticated, remote attacker to perform a stored cross-site scripting attack on an affected system. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need valid administrative credentials. Cisco expects to release software updates that address this vulnerability.	4.8	More Details
CVE-2021-24607	The Storefront Footer Text WordPress plugin through 1.0.1 does not sanitize and escape the "Footer Credit Text" added to pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered-html capability is disallowed.	4.8	More Details
CVE-2021-24708	The Export any WordPress data to XML/CSV WordPress plugin before 1.3.1 does not escape its Export's Name before outputting it in Manage Exports settings, 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 Number	Description	Base Score	Reference
CVE-2021-24616	The AddToAny Share Buttons WordPress plugin before 1.7.48 does not escape its Image URL button setting, which could lead allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-43032	In XenForo through 2.2.7, a threat actor with access to the admin panel can create a new Advertisement via the Advertising function, and save an XSS payload in the body of the HTML document. This payload will execute globally on the client side.	4.8	More Details
CVE-2021-24646	The Booking.com Banner Creator WordPress plugin before 1.4.3 does not properly sanitize inputs when creating banners, 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-2021-24664	The School Management System – WPSchoolPress WordPress plugin before 2.1.17 sanitise some fields using sanitize_text_field() but does not escape them before outputting in attributes, resulting in Stored Cross-Site Scripting issues.	4.8	More Details
CVE-2021-24701	The Quiz Tool Lite WordPress plugin through 2.3.15 does not sanitize multiple input fields used when creating or managing quizzes and in other setting options, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24706	The Qwizcards – online quizzes and flashcards WordPress plugin before 3.62 does not properly sanitize and escape some of its settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24645	The Booking.com Product Helper WordPress plugin before 1.0.2 does not sanitize and escape Product Code when creating Product Shortcode, 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-2020-27820	A vulnerability was found in Linux kernel, where a use-after-frees in nouveau's postclose() handler could happen if removing device (that is not common to remove video card physically without power-off, but same happens if "unbind" the driver).	4.7	More Details
CVE-2021-39237	Certain HP LaserJet, HP LaserJet Managed, HP PageWide, and HP PageWide Managed printers may be vulnerable to potential information disclosure.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39913	Accidental logging of system root password in the migration log in all versions of GitLab CE/EE before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 allows an attacker with local file system access to obtain system root-level privileges	4.4	More Details
CVE-2021-40126	A vulnerability in the web-based dashboard of Cisco Umbrella could allow an authenticated, remote attacker to perform an email enumeration attack against the Umbrella infrastructure. This vulnerability is due to an overly descriptive error message on the dashboard that appears when a user attempts to modify their email address when the new address already exists in the system. An attacker could exploit this vulnerability by attempting to modify the user's email address. A successful exploit could allow the attacker to enumerate email addresses of users in the system.	4.3	More Details
CVE-2021-24801	The WP Survey Plus WordPress plugin through 1.0 does not have any authorisation and CSRF checks in place in its AJAX actions, allowing any user to call them and add/edit/delete Surveys. Furthermore, due to the lack of sanitization in the Surveys' Title, this could also lead to Stored Cross-Site Scripting issues	4.3	More Details
CVE-2021-42026	A vulnerability has been identified in Mendix Applications using Mendix 8 (All versions < V8.18.13), Mendix Applications using Mendix 9 (All versions < V9.6.2). Applications built with affected versions of Mendix Studio Pro do not properly control read access for certain client actions. This could allow authenticated attackers to retrieve the changedDate attribute of arbitrary objects, even when they don't have read access to them.	4.3	More Details
CVE-2021-24816	The Phoenix Media Rename WordPress plugin before 3.4.4 does not have capability checks in its phoenix_media_rename AJAX action, which could allow users with Author roles to rename any uploaded media files, including ones they do not own.	4.3	More Details
CVE-2021-39905	An information disclosure vulnerability in the GitLab CE/EE API since version 8.9.6 allows a user to see basic information on private groups that a public project has been shared with	4.3	More Details
CVE-2021-39904	An Improper Access Control vulnerability in the GraphQL API in all versions of GitLab CE/EE starting from 13.1 before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 allows a Merge Request creator to resolve discussions and apply suggestions after a project owner has locked the Merge Request	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24806	The wpDiscuz WordPress plugin before 7.3.4 does check for CSRF when adding, editing and deleting comments, which could allow attacker to make logged in users such as admin edit and delete arbitrary comment, or the user who made the comment to edit it via a CSRF attack. Attackers could also make logged in users post arbitrary comment.	4.3	More Details
CVE-2021-24698	The Simple Download Monitor WordPress plugin before 3.9.6 allows users with a role as low as Contributor to remove thumbnails from downloads they do not own, even if they cannot normally edit the download.	4.3	More Details
CVE-2021-42663	An HTML injection vulnerability exists in Sourcecodester Online Event Booking and Reservation System in PHP/MySQL via the msg parameter to /event-management/index.php. An attacker can leverage this vulnerability in order to change the visibility of the website. Once the target user clicks on a given link he will display the content of the HTML code of the attacker's choice.	4.3	More Details
CVE-2021-41250	Python discord bot is the community bot for the Python Discord community. In affected versions when a non-blacklisted URL and an otherwise triggering filter token is included in the same message the token filter does not trigger. This means that by including any non-blacklisted URL moderation filters can be bypassed. This issue has been resolved in commit 67390298852513d13e0213870e50fb3cff1424e0	4.3	More Details
CVE-2021-31600	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. They implement a series of web services using the SOAP protocol to allow scripting interaction with the backend server. An authenticated user (regardless of privileges) can list all valid usernames.	4.3	More Details
CVE-2021-39902	Incorrect Authorization in GitLab CE/EE 13.4 or above allows a user with guest membership in a project to modify the severity of an incident.	4.3	More Details
CVE-2021-33210	An issue was discovered in Fimer Aurora Vision before 2.97.10. An attacker can (in the WebUI) obtain plant information without authentication by reading the response of APIs from a kiosk view of a plant.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34701	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), and Cisco Unity Connection could allow an authenticated, remote attacker to access sensitive data on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to access sensitive files on the affected system.	4.3	More Details
CVE-2021-43293	Sonatype Nexus Repository Manager 3.x before 3.36.0 allows a remote authenticated attacker to potentially perform network enumeration via Server Side Request Forgery (SSRF).	4.3	More Details
CVE-2021-24832	The WP SEO Redirect 301 WordPress plugin before 2.3.2 does not have CSRF in place when deleting redirects, which could allow attackers to make a logged in admin delete them via a CSRF attack	4.3	More Details
CVE-2021-25504	Intent redirection vulnerability in Group Sharing prior to 10.8.03.2 allows attacker to access contact information.	4.0	More Details
CVE-2021-25506	Non-existent provider in Samsung Health prior to 6.19.1.0001 allows attacker to access it via malicious content provider or lead to denial of service.	4.0	More Details
CVE-2021-39898	In all versions of GitLab CE/EE since version 10.6, a project export leaks the external webhook token value which may allow access to the project which it was exported from.	3.7	More Details
CVE-2021-41247	JupyterHub is an open source multi-user server for Jupyter notebooks. In affected versions users who have multiple JupyterLab tabs open in the same browser session, may see incomplete logout from the single-user server, as fresh credentials (for the single-user server only, not the Hub) reinstated after logout, if another active JupyterLab session is open while the logout takes place. Upgrade to JupyterHub 1.5. For distributed deployments, it is jupyterhub in the _user_ environment that needs patching. There are no patches necessary in the Hub environment. The only workaround is to make sure that only one JupyterLab tab is open when you log out.	3.5	More Details
CVE-2021-25505	Improper authentication in Samsung Pass prior to 3.0.02.4 allows to use app without authentication when lockscreen is unlocked.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23472	This affects versions before 1.19.1 of package bootstrap-table. A type confusion vulnerability can lead to a bypass of input sanitization when the input provided to the escapeHTML function is an array (instead of a string) even if the escape attribute is set.	3.1	More Details
CVE-2021-39914	A regular expression denial of service issue in GitLab versions 8.13 to 14.2.5, 14.3.0 to 14.3.3 and 14.4.0 could cause excessive usage of resources when a specially crafted username was used when provisioning a new user	3.1	More Details
CVE-2021-39901	In all versions of GitLab CE/EE since version 11.10, an admin of a group can see the SCIM token of that group by visiting a specific endpoint.	2.7	More Details
CVE-2021-34685	UploadService in Hitachi Vantara Pentaho Business Analytics through 9.1 does not properly verify uploaded user files, which allows an authenticated user to upload various files of different file types. Specifically, a .jsp file is not allowed, but a .jsp. file is allowed (and leads to remote code execution).	2.7	More Details
CVE-2021-39897	Improper access control in GitLab CE/EE version 10.5 and above allowed subgroup members with inherited access to a project from a parent group to still have access even after the subgroup is transferred	2.6	More Details
CVE-2021-39911	An improper access control flaw in all versions of GitLab CE/EE starting from 13.9 before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 exposes private email address of Issue and Merge Requests assignee to Webhook data consumers	1.7	More Details
CVE-2021-43338	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-43339. Reason: This candidate is a duplicate of CVE-2021-43339. Notes: All CVE users should reference CVE-2021-43339 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-23129	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-23130	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3896	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-43389. Reason: This candidate is a reservation duplicate of CVE-2021-43389. Notes: All CVE users should reference CVE-2021-43389 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details