SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 07 July 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-2021-28802	A command injection vulnerabilities have been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.1.1540 build 20210107. QNAP Systems Inc. QuTS hero versions prior to h4.5.1.1582 build 20210217.	9.8	More Details
CVE-2021-35474	Stack-based Buffer Overflow vulnerability in cachekey plugin of Apache Traffic Server. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1.	9.8	More Details
CVE-2021-24384	The joomsport_md_load AJAX action of the JoomSport WordPress plugin before 5.1.8, registered for both unauthenticated and unauthenticated users, unserialised user input from the shattr POST parameter, leading to a PHP Object Injection issue. Even though the plugin does not have a suitable gadget chain to exploit this, other installed plugins could, which might lead to more severe issues such as RCE	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24375	Lack of authentication or validation in motor_load_more, motor_gallery_load_more, motor_quick_view and motor_project_quick_view AJAX handlers of the Motor WordPress theme before 3.1.0 allows an unauthenticated attacker access to arbitrary files in the server file system, and to execute arbitrary php scripts found on the server file system. We found no vulnerability for uploading files with this theme, so any scripts to be executed must already be on the server file system.	9.8	More Details
CVE-2021-35209	An issue was discovered in ProxyServlet.java in the /proxy servlet in Zimbra Collaboration Suite 8.8 before 8.8.15 Patch 23 and 9.x before 9.0.0 Patch 16. The value of the X-Host header overwrites the value of the Host header in proxied requests. The value of X-Host header is not checked against the whitelist of hosts Zimbra is allowed to proxy to (the zimbraProxyAllowedDomains setting).	9.8	More Details
CVE-2021-36128	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. Autoblocks for CentralAuth-issued suppression blocks are not properly implemented.	9.8	More Details
CVE-2021-36126	An issue was discovered in the AbuseFilter extension in MediaWiki through 1.36. If the MediaWiki:Abusefilter-blocker message is invalid within the content language, the filter user falls back to the English version, but that English version could also be invalid on a wiki. This would result in a fatal error, and potentially fail to block or restrict a potentially nefarious user.	9.8	More Details
CVE-2021-35029	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device.	9.8	More Details
CVE-2021-35042	Django 3.1.x before 3.1.13 and 3.2.x before 3.2.5 allows QuerySet.order_by SQL injection if order_by is untrusted input from a client of a web application.	9.8	More Details
CVE-2021-35336	Tieline IP Audio Gateway 2.6.4.8 and below is affected by Incorrect Access Control. A vulnerability in the Tieline Web Administrative Interface could allow an unauthenticated user to access a sensitive part of the system with a high privileged account.	9.8	More Details
CVE-2021-36088	Fluent Bit (aka fluent-bit) 1.7.0 through 1.7.4 has a double free in flb_free (called from flb_parser_json_do and flb_parser_do).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36400	ZeroMQ libzmq 4.3.3 has a heap-based buffer overflow in zmq::tcp_read, a different vulnerability than CVE-2021-20235.	9.8	More Details
CVE-2018-25017	RawSpeed (aka librawspeed) 3.1 has a heap-based buffer overflow in TableLookUp::setTable.	9.8	More Details
CVE-2021-28804	A command injection vulnerabilities have been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.1.1540 build 20210107. QNAP Systems Inc. QuTS hero versions prior to h4.5.1.1582 build 20210217.	9.8	More Details
CVE-2020-22249	Remote Code Execution vulnerability in phplist 3.5.1. The application does not check any file extensions stored in the plugin zip file, Uploading a malicious plugin which contains the php files with extensions like PHP,phtml,php7 will be copied to the plugins directory which would lead to the remote code execution	9.8	More Details
CVE-2021-22345	There is an Input Verification Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause out-of-bounds memory write.	9.8	More Details
CVE-2021-22348	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause code to execute.	9.8	More Details
CVE-2021-22367	There is a Key Management Errors Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may lead to authentication bypass.	9.8	More Details
CVE-2021-35973	NETGEAR WAC104 devices before 1.0.4.15 are affected by an authentication bypass vulnerability in /usr/sbin/mini_httpd, allowing an unauthenticated attacker to invoke any action by adding the &currentsetting.htm substring to the HTTP query, a related issue to CVE-2020-27866. This directly allows the attacker to change the web UI password, and eventually to enable debug mode (telnetd) and gain a shell on the device as the admin limited-user account (however, escalation to root is simple because of weak permissions on the /etc/ directory).	9.8	More Details
CVE-2021-35971	Veeam Backup and Replication 10 before 10.0.1.4854 P20210609 and 11 before 11.0.0.837 P20210507 mishandles deserialization during Microsoft .NET remoting.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22323	There is an Integer Overflow Vulnerability in Huawei Smartphone. Successful exploitation of these vulnerabilities may escalate the permission to that of the root user.	9.8	More Details
CVE-2021-22375	There is a Key Management Errors Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality,availability and integrity.	9.8	More Details
CVE-2021-27903	An issue was discovered in Craft CMS before 3.6.7. In some circumstances, a potential Remote Code Execution vulnerability existed on sites that did not restrict administrative changes (if an attacker were somehow able to hijack an administrator's session).	9.8	More Details
CVE-2021-30648	The Symantec Advanced Secure Gateway (ASG) and ProxySG web management consoles are susceptible to an authentication bypass vulnerability. An unauthenticated attacker can execute arbitrary CLI commands, view/modify the appliance configuration and policy, and shutdown/restart the appliance.	9.8	More Details
CVE-2019-18906	A Improper Authentication vulnerability in cryptctl of SUSE Linux Enterprise Server for SAP 12-SP5, SUSE Manager Server 4.0 allows attackers with access to the hashed password to use it without having to crack it. This issue affects: SUSE Linux Enterprise Server for SAP 12-SP5 cryptctl versions prior to 2.4. SUSE Manager Server 4.0 cryptctl versions prior to 2.4.	9.8	More Details
CVE-2021-22354	There is an Information Disclosure Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause out-of-bounds read.	9.1	More Details
CVE-2021-22343	There is a Configuration Defect vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service integrity and availability.	9.1	More Details
CVE-2021-22373	There is a Defects Introduced in the Design Process Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service integrity and availability.	9.1	More Details
CVE-2021-22380	There is a Cleartext Transmission of Sensitive Information Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality and availability.	9.1	More Details
CVE-2021-35958	TensorFlow through 2.5.0 allows attackers to overwrite arbitrary files via a crafted archive when tf.keras.utils.get_file is used with extract=True. NOTE: the vendor's position is that tf.keras.utils.get_file is not intended for untrusted archives	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-36082	ntop nDPI 3.4 has a stack-based buffer overflow in processClientServerHello.	8.8	More Details
CVE-2021-36132	An issue was discovered in the FileImporter extension in MediaWiki through 1.36. For certain relaxed configurations of the $wgFileImporterRequiredRight variable, it might not validate all appropriate user rights, thus allowing a user with insufficient rights to perform operations (specifically file uploads) that they should not be allowed to perform.	8.8	More Details
CVE-2020-23219	Monstra CMS 3.0.4 allows attackers to execute arbitrary code via a crafted payload entered into the "Snippet content" field under the "Edit Snippet" module.	8.8	More Details
CVE-2021-36080	GNU LibreDWG 0.12.3.4163 through 0.12.3.4191 has a double-free in bit_chain_free (called from dwg_encode_MTEXT and dwg_encode_add_object).	8.8	More Details
CVE-2020-36407	libavif 0.8.0 and 0.8.1 has an out-of-bounds write in avifDecoderDataFillImageGrid.	8.8	More Details
CVE-2021-27950	A SQL injection vulnerability in azurWebEngine in Sita AzurCMS through 1.2.3.12 allows an authenticated attacker to execute arbitrary SQL commands via the id parameter to mesdocs.ajax.php in azurWebEngine/eShop. By default, the query is executed as DBA.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34527	A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. UPDATE July 7, 2021: The security update for Windows Server 2012, Windows Server 2016 and Windows 10, Version 1607 have been released. Please see the Security Updates table for the applicable update for your system. We recommend that you install these updates immediately. If you are unable to install these updates, see the FAQ and Workaround sections in this CVE for information on how to help protect your system from this vulnerability. In addition to installing the updates, in order to secure your system, you must confirm that the following registry settings are set to 0 (zero) or are not defined (Note: These registry keys do not exist by default, and therefore are already at the secure setting.), also that your Group Policy setting are correct (see FAQ): - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint - NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting) - UpdatePromptSettings = 0 (DWORD) or not defined (default setting) Having NoWarningNoElevationOnInstall set to 1 makes your system vulnerable by design. UPDATE July 6, 2021: Microsoft has completed the investigation and has released security updates to address this vulnerability. Please see the Security Updates table for the applicable update for your system. We recommend that you install these updates immediately. If you are unable to install these updates, see the FAQ and Workaround sections in this CVE for information on how to help protect your system from this vulnerability. See also KB5005010: Restricting installation of new printer drivers after applying the July 6, 2021 updates. Note that the security updates released on and after July 6, 2021 contain protections for CVE-2021-1675 and the additional remote code execution exploit in the Windows Print Spooler service known as “PrintNightmare”, documented in CVE-2021-34527.	8.8	More Details
CVE-2020-36406	uWebSockets 18.11.0 and 18.12.0 has a stack-based buffer overflow in uWS::TopicTree::trimTree (called from uWS::TopicTree::unsubscribeAll). NOTE: the vendor's position is that this is "a minor issue or not even an issue at all" because the developer of an application (that uses uWebSockets) should not be allowing the large number of triggered topics to accumulate	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27660	An insecure client auto update feature in C-CURE 9000 can allow remote execution of lower privileged Windows programs.	8.8	More Details
CVE-2021-30557	Use after free in TabGroups in Google Chrome prior to 91.0.4472.114 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30556	Use after free in WebAudio in Google Chrome prior to 91.0.4472.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30555	Use after free in Sharing in Google Chrome prior to 91.0.4472.114 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page and user gesture.	8.8	More Details
CVE-2020-27362	An issue exists within the SSH console of Akkadian Provisioning Manager 4.50.02 which allows a low-level privileged user to escape the web configuration file editor and escalate privileges.	8.8	More Details
CVE-2021-27661	Successful exploitation of this vulnerability could give an authenticated Facility Explorer SNC Series Supervisory Controller (F4-SNC) user an unintended level of access to the controller’s file system, allowing them to access or modify system files by sending specifically crafted web messages to the F4-SNC.	8.8	More Details
CVE-2020-36403	HTSlib through 1.10.2 allows out-of-bounds write access in vcf_parse_format (called from vcf_parse and vcf_read).	8.8	More Details
CVE-2020-4902	IBM Datacap Taskmaster Capture (IBM Datacap Navigator 9.1.7) is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 191045.	8.8	More Details
CVE-2021-28423	Multiple SQL Injection vulnerabilities in Teachers Record Management System 1.0 allow remote authenticated users to execute arbitrary SQL commands via the 'editid' GET parameter in edit-subjects-detail.php, edit-teacher-detail.php, or the 'searchdata' POST parameter in search.php.	8.8	More Details
CVE-2021-30554	Use after free in WebGL in Google Chrome prior to 91.0.4472.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32737	Sulu is an open-source PHP content management system based on the Symfony framework. In versions of Sulu prior to 1.6.41, it is possible for a logged in admin user to add a script injection (cross-site-scripting) in the collection title. The problem is patched in version 1.6.41. As a workaround, one may manually patch the affected JavaScript files in lieu of updating.	8.4	More Details
CVE-2021-22376	A component of the HarmonyOS has a Improper Privilege Management vulnerability. Local attackers may exploit this vulnerability to bypass user restrictions.	8.4	More Details
CVE-2021-22369	There is a Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability in Huawei Smartphone. Successful exploitation of these vulnerabilities may escalate the permission to that of the root user.	8.1	More Details
CVE-2021-22351	There is a Credentials Management Errors Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may induce users to grant permissions on modifying items in the configuration table,causing system exceptions.	8.1	More Details
CVE-2021-34373	Trusty trusted Linux kernel (TLK) contains a vulnerability in the NVIDIA TLK kernel where a lack of heap hardening could cause heap overflows, which might lead to information disclosure and denial of service.	7.9	More Details
CVE-2021-36081	Tesseract OCR 5.0.0-alpha-20201231 has a one_ell_conflict use-after-free during a strpbrk call.	7.8	More Details
CVE-2020-36401	mruby 2.1.2 has a double free in mrb_default_allocf (called from mrb_free and obj_free).	7.8	More Details
CVE-2020-36404	Keystone Engine 0.9.2 has an invalid free in llvm_ks::SmallVectorImpl<llvm_ks::MCFixup>::~SmallVectorImpl.	7.8	More Details
CVE-2020-36405	Keystone Engine 0.9.2 has a use-after-free in llvm_ks::X86Operand::getToken.	7.8	More Details
CVE-2021-3606	OpenVPN before version 2.5.3 on Windows allows local users to load arbitrary dynamic loadable libraries via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (openvpn.exe).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22352	There is a Configuration Defect Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may allow attackers to hijack the device and forge UIs to induce users to execute malicious commands.	7.8	More Details
CVE-2020-36402	Solidity 0.7.5 has a stack-use-after-return issue in smtutil::CHCSmtLib2Interface::querySolver. NOTE: c39a5e2b7a3fabbf687f53a2823fc087be6c1a7e is cited in the OSV "fixed" field but does not have a code change.	7.8	More Details
CVE-2021-27412	Delta Electronics DOPSoft Versions 4.0.10.17 and prior are vulnerable to an out-of-bounds read, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-3613	OpenVPN Connect 3.2.0 through 3.3.0 allows local users to load arbitrary dynamic loadable libraries via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (OpenVPNConnect.exe).	7.8	More Details
CVE-2021-36148	An issue was discovered in ACRN before 2.5. dmar_free_irte in hypervisor/arch/x86/vtd.c allows an irte_alloc_bitmap buffer overflow.	7.8	More Details
CVE-2018-25018	UnRAR 5.6.1.7 through 5.7.4 and 6.0.3 has an out-of-bounds write during a memcpy in QuickOpen::ReadRaw when called from QuickOpen::ReadNext.	7.8	More Details
CVE-2021-25321	A UNIX Symbolic Link (Symlink) Following vulnerability in arpwatch of SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Manager Server 4.0, SUSE OpenStack Cloud Crowbar 9; openSUSE Factory, Leap 15.2 allows local attackers with control of the runtime user to run arpwatch as to escalate to root upon the next restart of arpwatch. This issue affects: SUSE Linux Enterprise Server 11-SP4-LTSS arpwatch versions prior to 2.1a15. SUSE Manager Server 4.0 arpwatch versions prior to 2.1a15. SUSE OpenStack Cloud Crowbar 9 arpwatch versions prior to 2.1a15. openSUSE Factory arpwatch version 2.1a15-169.5 and prior versions. openSUSE Leap 15.2 arpwatch version 2.1a15-lp152.5.5 and prior versions.	7.8	More Details
CVE-2021-36089	Grok 7.6.6 through 9.2.0 has a heap-based buffer overflow in grk::FileFormatDecompress::apply_palette_clr (called from grk::FileFormatDecompress::applyColour).	7.8	More Details
CVE-2017-20006	UnRAR 5.6.1.2 and 5.6.1.3 has a heap-based buffer overflow in Unpack::CopyString (called from Unpack::Unpack5 and CmdExtract::ExtractCurrentFile).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35331	In Tcl 8.6.11, a format string vulnerability in nmakehlp.c might allow code execution via a crafted file. NOTE: multiple third parties dispute the significance of this finding	7.8	More Details
CVE-2021-34379	Trusty contains a vulnerability in the HDCP service TA where bounds checking in command 10 is missing. The length of an I/O buffer parameter is not checked, which might lead to memory corruption.	7.7	More Details
CVE-2021-34374	Trusty contains a vulnerability in command handlers where the length of input buffers is not verified. This vulnerability can cause memory corruption, which may lead to information disclosure, escalation of privileges, and denial of service.	7.7	More Details
CVE-2021-34375	Trusty contains a vulnerability in all trusted applications (TAs) where the stack cookie was not randomized, which might result in stack-based buffer overflow, leading to denial of service, escalation of privileges, and information disclosure.	7.7	More Details
CVE-2021-34376	Trusty contains a vulnerability in the HDCP service TA where bounds checking in command 5 is missing. Improper restriction of operations within the bounds of a memory buffer might lead to denial of service, escalation of privileges, and information disclosure.	7.7	More Details
CVE-2021-34377	Trusty contains a vulnerability in the HDCP service TA where bounds checking in command 9 is missing. Improper restriction of operations within the bounds of a memory buffer might lead to escalation of privileges, information disclosure, and denial of service.	7.7	More Details
CVE-2021-34378	Trusty contains a vulnerability in the HDCP service TA where bounds checking in command 11 is missing. Improper restriction of operations within the bounds of a memory buffer might lead to information disclosure, denial of service, or escalation of privileges.	7.7	More Details
CVE-2021-35197	In MediaWiki before 1.31.15, 1.32.x through 1.35.x before 1.35.3, and 1.36.x before 1.36.1, bots have certain unintended API access. When a bot account has a "sitewide block" applied, it is able to still "purge" pages through the MediaWiki Action API (which a "sitewide block" should have prevented).	7.5	More Details
CVE-2021-28127	An issue was discovered in Stormshield SNS through 4.2.1. A brute-force attack can occur.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36125	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. The Special:GlobalRenameRequest page is vulnerable to infinite loops and denial of service attacks when a user's current username is beyond an arbitrary maximum configuration value (MaxNameChars).	7.5	More Details
CVE-2021-27477	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop.	7.5	More Details
CVE-2020-26763	The Rocket.Chat desktop application 2.17.11 opens external links without user interaction.	7.5	More Details
CVE-2020-9158	There is a Missing Cryptographic Step vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause DoS of Samgr.	7.5	More Details
CVE-2021-20778	Improper access control vulnerability in EC-CUBE 4.0.6 (EC-CUBE 4 series) allows a remote attacker to bypass access restriction and obtain sensitive information via unspecified vectors.	7.5	More Details
CVE-2021-36147	An issue was discovered in ACRN before 2.5. It allows a devicemodel/hw/pci/virtio/virtio_net.c virtio_net_ping_rxq NULL pointer dereference for vq->used.	7.5	More Details
CVE-2021-32566	Improper Input Validation vulnerability in HTTP/2 of Apache Traffic Server allows an attacker to DOS the server. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1.	7.5	More Details
CVE-2021-32736	think-helper defines a set of helper functions for ThinkJS. In versions of think-helper prior to 1.1.3, the software receives input from an upstream component that specifies attributes that are to be initialized or updated in an object, but it does not properly control modifications of attributes of the object prototype. The vulnerability is patched in version 1.1.3.	7.5	More Details
CVE-2021-36146	ACRN before 2.5 has a devicemodel/hw/pci/xhci.c NULL Pointer Dereference for a trb pointer.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21671	Jenkins 2.299 and earlier, LTS 2.289.1 and earlier does not invalidate the previous session on login.	7.5	More Details
CVE-2021-32567	Improper Input Validation vulnerability in HTTP/2 of Apache Traffic Server allows an attacker to DOS the server. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1.	7.5	More Details
CVE-2021-25951	XXE vulnerability in 'XML2Dict' version 0.2.2 allows an attacker to cause a denial of service.	7.5	More Details
CVE-2021-28993	Plixer Scrutinizer 19.0.2 is affected by: SQL Injection. The impact is: obtain sensitive information (remote).	7.5	More Details
CVE-2021-36143	ACRN before 2.5 has a hw/pci/virtio/virtio.c vq_endchains NULL Pointer Dereference.	7.5	More Details
CVE-2021-22370	There is a Credentials Management Errors Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-22372	There is a Security Features Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-36145	The Device Model in ACRN through 2.5 has a devicemodel/core/mem.c use-after-free for a freed rb_entry.	7.5	More Details
CVE-2021-22371	There is an Improper Permission Management Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-22374	There is an Improper Validation of Array Index Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause stability risks.	7.5	More Details
CVE-2021-35970	Talk 4 in Coral before 4.12.1 allows remote attackers to discover e-mail addresses and other sensitive information via GraphQL because permission checks use an incorrect data type.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27361	An issue exists within Akkadian Provisioning Manager 4.50.02 which allows attackers to view sensitive information within the /pme subdirectories.	7.5	More Details
CVE-2021-22350	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause the device to crash and restart.	7.5	More Details
CVE-2021-22349	There is an Input Verification Vulnerability in Huawei Smartphone. Successful exploitation of insufficient input verification may cause the system to restart.	7.5	More Details
CVE-2021-36144	The polling timer handler in ACRN before 2.5 has a use-after-free for a freed virtio device, related to devicemodel/hw/pci/virtio/*.c.	7.5	More Details
CVE-2021-22353	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause the kernel to restart.	7.5	More Details
CVE-2021-22368	There is a Permission Control Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect normal use of the device.	7.5	More Details
CVE-2021-32740	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. An uncontrolled resource consumption vulnerability exists after version 2.3.0 through version 2.7.0. Within the URI template implementation in Addressable, a maliciously crafted template may result in uncontrolled resource consumption, leading to denial of service when matched against a URI. In typical usage, templates would not normally be read from untrusted user input, but nonetheless, no previous security advisory for Addressable has cautioned against doing this. Users of the parsing capabilities in Addressable but not the URI template capabilities are unaffected. The vulnerability is patched in version 2.8.0. As a workaround, only create Template objects from trusted sources that have been validated not to produce catastrophic backtracking.	7.5	More Details
CVE-2021-23402	All versions of package record-like-deep-assign are vulnerable to Prototype Pollution via the main functionality.	7.3	More Details
CVE-2021-23403	All versions of package ts-nodash are vulnerable to Prototype Pollution via the Merge() function due to lack of validation input.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32639	Emissary is a P2P-based, data-driven workflow engine. Emissary version 6.4.0 is vulnerable to Server-Side Request Forgery (SSRF). In particular, the `RegisterPeerAction` endpoint and the `AddChildDirectoryAction` endpoint are vulnerable to SSRF. This vulnerability may lead to credential leaks. Emissary version 7.0 contains a patch. As a workaround, disable network access to Emissary from untrusted sources.	7.2	More Details
CVE-2021-24451	The Export Users With Meta WordPress plugin before 0.6.5 did not escape the list of roles to export before using them in a SQL statement in the export functionality, available to admins, leading to an authenticated SQL Injection.	7.2	More Details
CVE-2021-22326	A component of the HarmonyOS has a Privilege Dropping / Lowering Errors vulnerability. Local attackers may exploit this vulnerability to obtain Kernel space read/write capability.	7.1	More Details
CVE-2021-32735	Kirby is a content management system. In Kirby CMS versions 3.5.5 and 3.5.6, the Panel's `ListItem` component (used in the pages and files section for example) displayed HTML in page titles as it is. This could be used for cross-site scripting (XSS) attacks. Malicious authenticated Panel users can escalate their privileges if they get access to the Panel session of an admin user. Visitors without Panel access can use the attack vector if the site allows changing site data from a frontend form. Kirby 3.5.7 patches the vulnerability. As a partial workaround, site administrators can protect against attacks from visitors without Panel access by validating or sanitizing provided data from the frontend form.	7.1	More Details
CVE-2019-25049	LibreSSL 2.9.1 through 3.2.1 has an out-of-bounds read in asn1_item_print_ctx (called from asn1_template_print_ctx).	7.1	More Details
CVE-2021-28692	inappropriate x86 IOMMU timeout detection / handling IOMMUs process commands issued to them in parallel with the operation of the CPU(s) issuing such commands. In the current implementation in Xen, asynchronous notification of the completion of such commands is not used. Instead, the issuing CPU spin-waits for the completion of the most recently issued command(s). Some of these waiting loops try to apply a timeout to fail overly-slow commands. The course of action upon a perceived timeout actually being detected is inappropriate: - on Intel hardware guests which did not originally cause the timeout may be marked as crashed, - on AMD hardware higher layer callers would not be notified of the issue, making them continue as if the IOMMU operation succeeded.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25048	LibreSSL 2.9.1 through 3.2.1 has a heap-based buffer over-read in do_print_ex (called from asn1_item_print_ctx and ASN1_item_print).	7.1	More Details
CVE-2021-34380	Bootloader contains a vulnerability in NVIDIA MB2 where potential heap overflow might cause corruption of the heap metadata, which might lead to arbitrary code execution, denial of service, and information disclosure during secure boot.	7.0	More Details
CVE-2021-33889	OpenThread wpantund through 2021-07-02 has a stack-based Buffer Overflow because of an inconsistency in the integer data type for metric_len.	6.8	More Details
CVE-2021-34382	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel's tz_map_shared_mem function where an integer overflow on the size parameter causes the request buffer and the logging buffer to overflow, allowing writes to arbitrary addresses within the kernel.	6.7	More Details
CVE-2021-34381	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel function where a lack of checks allows the exploitation of an integer overflow on the size parameter of the tz_map_shared_mem function, which might lead to denial of service, information disclosure, or data tampering.	6.7	More Details
CVE-2021-26920	In the Druid ingestion system, the InputSource is used for reading data from a certain data source. However, the HTTP InputSource allows authenticated users to read data from other sources than intended, such as the local file system, with the privileges of the Druid server process. This is not an elevation of privilege when users access Druid directly, since Druid also provides the Local InputSource, which allows the same level of access. But it is problematic when users interact with Druid indirectly through an application that allows users to specify the HTTP InputSource, but not the Local InputSource. In this case, users could bypass the application-level restriction by passing a file URL to the HTTP InputSource.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32738	js-stellar-sdk is a Javascript library for communicating with a Stellar Horizon server. The `Utils.readChallengeTx` function used in SEP-10 Stellar Web Authentication states in its function documentation that it reads and validates the challenge transaction including verifying that the `serverAccountID` has signed the transaction. In js-stellar-sdk before version 8.2.3, the function does not verify that the server has signed the transaction. Applications that also used `Utils.verifyChallengeTxThreshold` or `Utils.verifyChallengeTxSigners` to verify the signatures including the server signature on the challenge transaction are unaffected as those functions verify the server signed the transaction. Applications calling `Utils.readChallengeTx` should update to version 8.2.3, the first version with a patch for this vulnerability, to ensure that the challenge transaction is completely valid and signed by the server creating the challenge transaction.	6.5	More Details
CVE-2021-22228	An issue has been discovered in GitLab affecting all versions before 13.11.6, all versions starting from 13.12 before 13.12.6, and all versions starting from 14.0 before 14.0.2. Improper access control allows unauthorised users to access project details using Graphql.	6.5	More Details
CVE-2021-21675	A cross-site request forgery (CSRF) vulnerability in Jenkins requests-plugin Plugin 2.2.12 and earlier allows attackers to create requests and/or have administrators apply pending requests.	6.5	More Details
CVE-2021-20461	IBM Cognos Analytics 10.0 and 11.1 is susceptible to a weakness in the implementation of the System Appearance configuration setting. An attacker could potentially bypass business logic to modify the appearance and behavior of the application. IBM X-Force ID: 196770.	6.5	More Details
CVE-2021-24405	The Easy Cookies Policy WordPress plugin through 1.6.2 is lacking any capability and CSRF check when saving its settings, allowing any authenticated users (such as subscriber) to change them. If users can't register, this can be done through CSRF. Furthermore, the cookie banner setting is not sanitised or validated before being output in all pages of the frontend and the backend settings one, leading to a Stored Cross-Site Scripting issue.	6.5	More Details
CVE-2021-32559	An integer overflow exists in pywin32 prior to version b301 when adding an access control entry (ACE) to an access control list (ACL) that would cause the size to be greater than 65535 bytes. An attacker who successfully exploited this vulnerability could crash the vulnerable process.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22226	Under certain conditions, some users were able to push to protected branches that were restricted to deploy keys in GitLab CE/EE since version 13.9	6.5	More Details
CVE-2021-34383	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might lead to denial of service or escalation of privileges.	6.4	More Details
CVE-2021-34384	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow could cause memory corruption, which might lead to denial of service or code execution.	6.3	More Details
CVE-2021-34385	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel where an integer overflow in the calculation of a length could lead to a heap overflow.	6.3	More Details
CVE-2020-36194	An XSS vulnerability has been reported to affect QNAP NAS running QTS and QuTS hero. If exploited, this vulnerability allows attackers to inject malicious code. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.2.1566 Build 20210202. QNAP Systems Inc. QuTS hero versions prior to h4.5.2.1638 build 20210414. This issue does not affect: QNAP Systems Inc. QTS 4.5.3.	6.1	More Details
CVE-2021-35440	Smashing 1.3.4 is vulnerable to Cross Site Scripting (XSS). A URL for a widget can be crafted and used to execute JavaScript on the victim's computer. The JavaScript code can then steal data available in the session/cookies depending on the user environment (e.g. if re-using internal URL's for deploying, or cookies that are very permissive) private information may be retrieved by the attacker.	6.1	More Details
CVE-2021-21673	Jenkins CAS Plugin 1.6.0 and earlier improperly determines that a redirect URL after login is legitimately pointing to Jenkins, allowing attackers to perform phishing attacks.	6.1	More Details
CVE-2021-22223	Client-Side code injection through Feature Flag name in GitLab CE/EE starting with 11.9 allows a specially crafted feature flag name to PUT requests on behalf of other users via clicking on a link	6.1	More Details
CVE-2021-35207	An issue was discovered in Zimbra Collaboration Suite 8.8 before 8.8.15 Patch 23 and 9.0 before 9.0.0 Patch 16. An XSS vulnerability exists in the login component of Zimbra Web Client, in which an attacker can execute arbitrary JavaScript by adding executable JavaScript to the loginErrorCode parameter of the login url.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34807	An open redirect vulnerability exists in the /preauth Servlet in Zimbra Collaboration Suite through 9.0. To exploit the vulnerability, an attacker would need to have obtained a valid zimbra auth token or a valid preauth token. Once the token is obtained, an attacker could redirect a user to any URL via isredirect=1&redirectURL= in conjunction with the token data (e.g., a valid authtoken= value).	6.1	More Details
CVE-2021-27902	An issue was discovered in Craft CMS before 3.6.0. In some circumstances, a potential XSS vulnerability existed in connection with front-end forms that accepted user uploads.	6.1	More Details
CVE-2021-31721	Chevereto before 3.17.1 allows Cross Site Scripting (XSS) via an image title at the image upload stage.	6.1	More Details
CVE-2020-36196	A stored XSS vulnerability has been reported to affect QNAP NAS running QuLog Center. If exploited, this vulnerability allows attackers to inject malicious code. This issue affects: QNAP Systems Inc. QuLog Center versions prior to 1.2.0.	6.1	More Details
CVE-2021-24387	The WP Pro Real Estate 7 WordPress theme before 3.1.1 did not properly sanitise the ct_community parameter in its search listing page before outputting it back in it, leading to a reflected Cross-Site Scripting which can be triggered in both unauthenticated or authenticated user context	6.1	More Details
CVE-2021-24406	The wpForo Forum WordPress plugin before 1.9.7 did not validate the redirect_to parameter in the login form of the forum, leading to an open redirect issue after a successful login. Such issue could allow an attacker to induce a user to use a login URL redirecting to a website under their control and being a replica of the legitimate one, asking them to re-enter their credentials (which will then in the attacker hands)	6.1	More Details
CVE-2021-20752	Cross-site scripting vulnerability in Ikaika RSS Reader all versions allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-24389	The WP Foodbakery WordPress plugin before 2.2, used in the FoodBakery WordPress theme before 2.2 did not properly sanitize the foodbakery_radius parameter before outputting it back in the response, leading to an unauthenticated Reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-32233	SmarterTools SmarterMail before Build 7776 allows XSS.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33192	A vulnerability in the HTML pages of Apache Jena Fuseki allows an attacker to execute arbitrary javascript on certain page views. This issue affects Apache Jena Fuseki from version 2.0.0 to version 4.0.0 (inclusive).	6.1	More Details
CVE-2021-24407	The Jannah WordPress theme before 5.4.5 did not properly sanitize the 'query' POST parameter in its tie_ajax_search AJAX action, leading to a Reflected Cross-site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-31874	Zoho ManageEngine ADSelfService Plus before 6104, in rare situations, allows attackers to obtain sensitive information about the password-sync database application.	5.9	More Details
CVE-2021-36158	In the xrdp package (in branches through 3.14) for Alpine Linux, RDP sessions are vulnerable to man-in-the-middle attacks because pre-generated RSA certificates and private keys are used.	5.9	More Details
CVE-2021-22229	An issue has been discovered in GitLab CE/EE affecting all versions starting with 12.8. Under a special condition it was possible to access data of an internal repository through project fork done by a project member.	5.9	More Details
CVE-2021-34075	In Artica Pandora FMS <=754 in the File Manager component, there is sensitive information exposed on the client side which attackers can access.	5.9	More Details
CVE-2021-32730	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A cross-site request forgery vulnerability exists in versions prior to 12.10.5, and in versions 13.0 through 13.1. It's possible for forge an URL that, when accessed by an admin, will reset the password of any user in XWiki. The problem has been patched in XWiki 12.10.5 and 13.2RC1. As a workaround, it is possible to apply the patch manually by modifying the `register_macros.vm` template.	5.7	More Details
CVE-2021-3598	There's a flaw in OpenEXR's ImfDeepScanLineInputFile functionality in versions prior to 3.0.5. An attacker who is able to submit a crafted file to an application linked with OpenEXR could cause an out-of-bounds read. The greatest risk from this flaw is to application availability.	5.5	More Details
CVE-2021-3630	An out-of-bounds write vulnerability was found in DjVuLibre in DJVU::DjVuTXT::decode() in DjVuText.cpp via a crafted djvu file which may lead to crash and segmentation fault. This flaw affects DjVuLibre versions prior to 3.5.28.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28693	xen/arm: Boot modules are not scrubbed The bootloader will load boot modules (e.g. kernel, initramfs...) in a temporary area before they are copied by Xen to each domain memory. To ensure sensitive data is not leaked from the modules, Xen must "scrub" them before handing the page over to the allocator. Unfortunately, it was discovered that modules will not be scrubbed on Arm.	5.5	More Details
CVE-2021-36083	KDE KImageFormats 5.70.0 through 5.81.0 has a stack-based buffer overflow in XCFImageFormat::loadTileRLE.	5.5	More Details
CVE-2021-27455	Delta Electronics DOPSoft Versions 4.0.10.17 and prior are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to disclose information.	5.5	More Details
CVE-2020-36416	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Create a new Design" parameter under the "Designs" module.	5.4	More Details
CVE-2020-36415	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Create a new Stylesheet" parameter under the "Stylesheets" module.	5.4	More Details
CVE-2020-36414	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "URL (slug)" or "Extra" fields under the "Add Article" feature.	5.4	More Details
CVE-2020-36412	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Search Text" field under the "Admin Search" module.	5.4	More Details
CVE-2021-24388	In the VikRentCar Car Rental Management System WordPress plugin before 1.1.7, there is a custom filed option by which we can manage all the fields that the users will have to fill in before saving the order. However, the field name is not sanitised or escaped before being output back in the page, leading to a stored Cross-Site Scripting issue. There is also no CSRF check done before saving the setting, allowing attackers to make a logged in admin set arbitrary Custom Fields, including one with XSS payload in it.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23401	This affects all versions of package Flask-User. When using the make_safe_url function, it is possible to bypass URL validation and redirect a user to an arbitrary URL by providing multiple back slashes such as /////evil.com/path or \\\evil.com/path. This vulnerability is only exploitable if an alternative WSGI server other than Werkzeug is used, or the default behaviour of Werkzeug is modified using 'autocorrect_location_header=False.	5.4	More Details
CVE-2021-35208	An issue was discovered in ZmMailMsgView.js in the Calendar Invite component in Zimbra Collaboration Suite 8.8.x before 8.8.15 Patch 23. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document.	5.4	More Details
CVE-2020-23697	Cross Site Scripting vulnerabilty in Monstra CMS 3.0.4 via the page feature in admin/index.php.	5.4	More Details
CVE-2021-24494	The WP Offload SES Lite WordPress plugin before 1.4.5 did not escape some of the fields in the Activity page of the admin dashboard, such as the email's id, subject and recipient, which could lead to Stored Cross-Site Scripting issues when an attacker can control any of these fields, like the subject when filling a contact form for example. The XSS will be executed in the context of a logged in admin viewing the Activity tab of the plugin.	5.4	More Details
CVE-2021-24386	The WP SVG images WordPress plugin before 3.4 did not sanitise the SVG files uploaded, which could allow low privilege users such as author+ to upload a malicious SVG and then perform XSS attacks by inducing another user to access the file directly. In v3.4, the plugin restricted such upload to editors and admin, with an option to also allow author to do so. The description of the plugin has also been updated with a security warning as upload of such content is intended.	5.4	More Details
CVE-2021-27930	Multiple stored XSS vulnerabilities in IrisNext Edition 9.5.16, which allows an authenticated (or compromised) user to inject malicious JavaScript in folder/file name within the application in order to grab other users' sessions or execute malicious code in their browsers (1-click RCE).	5.4	More Details
CVE-2020-36413	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Exclude these IP addresses from the "Site Down" status" parameter under the "Maintenance Mode" module.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35959	In Plone 5.0 through 5.2.4, Editors are vulnerable to XSS in the folder contents view, if a Contributor has created a folder with a SCRIPT tag in the description field.	5.4	More Details
CVE-2020-36411	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Path for the {page_image} tag:" or "Path for thumbnail field:" parameters under the "Content Editing Settings" module.	5.4	More Details
CVE-2020-23181	A reflected cross site scripting (XSS) vulnerability in /administration/theme.php of PHP-Fusion 9.03.60 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Manage Theme" field.	5.4	More Details
CVE-2021-35956	Stored cross-site scripting (XSS) in the embedded webserver of AKCP sensorProbe before SP480-20210624 enables remote authenticated attackers to introduce arbitrary JavaScript via the Sensor Description, Email (from/to/cc), System Name, and System Location fields.	5.4	More Details
CVE-2021-20107	There exists an unauthenticated BLE Interface in Sloan SmartFaucets including Optima EAF, Optima ETF/EBF, BASYS EFX, and Flushometers including SOLIS. The vulnerability allows for unauthenticated kinetic effects and information disclosure on the faucets. It is possible to use the Bluetooth Low Energy (BLE) connectivity to read and write to many BLE characteristics on the device. Some of these control the flow of water, the sensitivity of the sensors, and information about maintenance.	5.4	More Details
CVE-2021-28803	This issue affects: QNAP Systems Inc. Q'center versions prior to 1.11.1004.	5.4	More Details
CVE-2021-31813	Zoho ManageEngine Applications Manager before 15130 is vulnerable to Stored XSS while importing malicious user details (e.g., a crafted user name) from AD.	5.4	More Details
CVE-2021-28424	A stored cross-site scripting (XSS) vulnerability in Teachers Record Management System 1.0 allows remote authenticated users to inject arbitrary web script or HTML via the 'email' POST parameter in adminprofile.php.	5.4	More Details
CVE-2020-4935	IBM Datacap Fastdoc Capture (IBM Datacap Navigator 9.1.7) 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: 191753.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36410	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Email address to receive notification of news submission" parameter under the "Options" module.	5.4	More Details
CVE-2020-23208	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Send test" field under the "Start or continue campaign" module.	5.4	More Details
CVE-2020-23209	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "List Description" field under the "Edit A List" module.	5.4	More Details
CVE-2020-23214	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Configure categories" field under the "Categorise Lists" module.	5.4	More Details
CVE-2020-23217	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Add a list" field under the "Import Emails" module.	5.4	More Details
CVE-2020-23178	An issue exists in PHP-Fusion 9.03.50 where session cookies are not deleted once a user logs out, allowing for an attacker to perform a session replay attack and impersonate the victim user.	5.4	More Details
CVE-2020-23179	A stored cross site scripting (XSS) vulnerability in administration/settings_main.php of PHP-Fusion 9.03.50 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Site footer" field.	5.4	More Details
CVE-2020-23207	A stored cross site scripting (XSS) vulnerability in phplist 3.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Edit Values" field under the "Configure Attributes" module.	5.4	More Details
CVE-2020-23182	The component /php-fusion/infusions/shoutbox_panel/shoutbox_archive.php in PHP-Fusion 9.03.60 allows attackers to redirect victim users to malicious websites via a crafted payload entered into the Shoutbox message panel.	5.4	More Details
CVE-2020-36395	A stored cross site scripting (XSS) vulnerability in the /admin/user/team component of LavaLite 5.8.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "New" parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36409	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Add Category" parameter under the "Categories" module.	5.4	More Details
CVE-2020-36408	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Add Shortcut" parameter under the "Manage Shortcuts" module.	5.4	More Details
CVE-2020-36399	A stored cross site scripting (XSS) vulnerability in phplist 3.5.4 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the "rule1" parameter under the "Bounce Rules" module.	5.4	More Details
CVE-2020-23184	A stored cross site scripting (XSS) vulnerability in /administration/settings_registration.php of PHP-Fusion 9.03.60 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Registration" field.	5.4	More Details
CVE-2020-36398	A stored cross site scripting (XSS) vulnerability in phplist 3.5.4 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the "Campaign" field under the "Send a campaign" module.	5.4	More Details
CVE-2020-36397	A stored cross site scripting (XSS) vulnerability in the /admin/contact/contact component of LavaLite 5.8.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "New" parameter.	5.4	More Details
CVE-2020-36396	A stored cross site scripting (XSS) vulnerability in the /admin/roles/role component of LavaLite 5.8.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "New" parameter.	5.4	More Details
CVE-2020-23205	A stored cross site scripting (XSS) vulnerability in Monstra CMS version 3.0.4 allows attackers to execute arbitrary web scripts or HTML via crafted a payload entered into the "Site Name" field under the "Site Settings" module.	5.4	More Details
CVE-2020-23194	A stored cross site scripting (XSS) vulnerability in the "Import Subscribers" feature in phplist 3.5.4 and below allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2020-23185	A stored cross site scripting (XSS) vulnerability in /administration/setting_security.php of PHP-Fusion 9.03.60 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23192	A stored cross site scripting (XSS) vulnerability in phplist 3.5.4 and below allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload in the "admin" parameter under the "Manage administrators" module.	5.4	More Details
CVE-2020-23190	A stored cross site scripting (XSS) vulnerability in the "Import emails" module in phplist 3.5.4 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2021-22346	There is an Improper Permission Management Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may lead to the disclosure of user habits.	5.3	More Details
CVE-2021-32731	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Between (and including) versions 13.1RC1 and 13.1, the reset password form reveals the email address of users just by giving their username. The problem has been patched on XWiki 13.2RC1. As a workaround, it is possible to manually modify the `resetpasswordinline.vm` to perform the changes made to mitigate the vulnerability.	5.3	More Details
CVE-2021-22347	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause temporary DoS.	5.3	More Details
CVE-2021-22344	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause temporary DoS.	5.3	More Details
CVE-2021-36131	An XSS issue was discovered in the SportsTeams extension in MediaWiki through 1.36. Within several special pages, a privileged user could inject arbitrary HTML and JavaScript within various data fields. The attack could easily propagate across many pages for many users.	4.8	More Details
CVE-2021-36130	An XSS issue was discovered in the SocialProfile extension in MediaWiki through 1.36. Within several gift-related special pages, a privileged user with the awardmanage right could inject arbitrary HTML and JavaScript within various gift-related data fields. The attack could easily propagate across many pages for many users.	4.8	More Details
CVE-2020-22251	Cross Site Scripting (XSS) vulnerability in phpList 3.5.3 via the login name field in Manage Administrators when adding a new admin.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34190	A stored cross site scripting (XSS) vulnerability in index.php?menu=billing_rates of Issabel PBX version 4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Name" or "Prefix" fields under the "Create New Rate" module.	4.8	More Details
CVE-2021-36127	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. The Special:GlobalUserRights page provided search results which, for a suppressed MediaWiki user, were different than for any other user, thus easily disclosing suppressed accounts (which are supposed to be completely hidden).	4.3	More Details
CVE-2021-35337	Sourcecodester Phone Shop Sales Managements System 1.0 is vulnerable to Insecure Direct Object Reference (IDOR). Any attacker will be able to see the invoices of different users by changing the id parameter.	4.3	More Details
CVE-2021-21670	Jenkins 2.299 and earlier, LTS 2.289.1 and earlier allows users to cancel queue items and abort builds of jobs for which they have Item/Cancel permission even when they do not have Item/Read permission.	4.3	More Details
CVE-2021-21672	Jenkins Selenium HTML report Plugin 1.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	4.3	More Details
CVE-2021-21674	A missing permission check in Jenkins requests-plugin Plugin 2.2.6 and earlier allows attackers with Overall/Read permission to view the list of pending requests.	4.3	More Details
CVE-2021-21676	Jenkins requests-plugin Plugin 2.2.7 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to send test emails to an attacker-specified email address.	4.3	More Details
CVE-2021-36129	An issue was discovered in the Translate extension in MediaWiki through 1.36. The Aggregategroups Action API module does not validate the parameter for aggregategroup when action=remove is set, thus allowing users with the translate-manage right to silently delete various groups' metadata.	4.3	More Details
CVE-2021-24005	Usage of hard-coded cryptographic keys to encrypt configuration files and debug logs in FortiAuthenticator versions before 6.3.0 may allow an attacker with access to the files or the CLI configuration to decrypt the sensitive data, via knowledge of the hard-coded key.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22232	HTML injection was possible via the full name field before versions 13.11.6, 13.12.6, and 14.0.2 in GitLab CE	3.5	More Details
CVE-2021-36085	The CIL compiler in SELinux 3.2 has a use-after-free in __cil_verify_classperms (called from __verify_map_perm_classperms and hashtab_map).	3.3	More Details
CVE-2021-36086	The CIL compiler in SELinux 3.2 has a use-after-free in cil_reset_classpermission (called from cil_reset_classperms_set and cil_reset_classperms_list).	3.3	More Details
CVE-2021-36087	The CIL compiler in SELinux 3.2 has a heap-based buffer over-read in ebitmap_match_any (called indirectly from cil_check_neverallow). This occurs because there is sometimes a lack of checks for invalid statements in an optional block.	3.3	More Details
CVE-2021-36084	The CIL compiler in SELinux 3.2 has a use-after-free in __cil_verify_classperms (called from __cil_verify_classpermission and __cil_pre_verify_helper).	3.3	More Details
CVE-2021-32729	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A vulnerability exists in versions prior to 12.6.88, 12.10.4, and 13.0. The script service method used to reset the authentication failures record can be executed by any user with Script rights and does not require Programming rights. An attacher with script rights who is able to reset the authentication failure record might perform a brute force attack, since they would be able to virtually deactivate the mechanism introduced to mitigate those attacks. The problem has been patched in version 12.6.8, 12.10.4 and 13.0. There are no workarounds aside from upgrading.	2.0	More Details
CVE-2021-31771	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