SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 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-2019-19810	Zoom Call Recording 6.3.1 from Eleveo is vulnerable to Java Deserialization attacks targeting the inbuilt RMI service. A remote unauthenticated attacker can exploit this vulnerability by sending crafted RMI requests to execute arbitrary code on the target host.	10.0	More Details
CVE-2021-38450	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software.	9.9	More Details
CVE-2011-4124	Input validation issues were found in Calibre at devices/linux_mount_helper.c which can lead to argument injection and elevation of privileges.	9.8	More Details
CVE-2021-29212	A remote unauthenticated directory traversal security vulnerability has been identified in HPE iLO Amplifier Pack versions 1.80, 1.81, 1.90 and 1.95. The vulnerability could be remotely exploited to allow an unauthenticated user to run arbitrary code leading complete impact to confidentiality, integrity, and availability of the iLO Amplifier Pack appliance.	9.8	More Details
CVE-2011-4125	A untrusted search path issue was found in Calibre at devices/linux_mount_helper.c leading to the ability of unprivileged users to execute any program as root.	9.8	More Details
CVE-2020-26707	An issue was discovered in the add function in Shenzhim AAPTJS 1.3.1 which allows attackers to execute arbitrary code via the filePath parameter.	9.8	More Details
CVE-2020-36376	An issue was discovered in the list function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	9.8	More Details
CVE-2020-36377	An issue was discovered in the dump function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	9.8	More Details
CVE-2020-36378	An issue was discovered in the packageCmd function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	9.8	More Details
CVE-2020-36379	An issue was discovered in the remove function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	9.8	More Details
CVE-2020-36380	An issue was discovered in the crunch function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	9.8	More Details
CVE-2020-36381	An issue was discovered in the singleCrunch function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	9.8	More Details
CVE-2021-3705	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow an unauthorized user to reconfigure, reset the device.	9.8	More Details
CVE-2021-41644	Remote Code Exection (RCE) vulnerability exists in Sourcecodester Online Food Ordering System 2.0 via a maliciously crafted PHP file that bypasses the image upload filters.	9.8	More Details
CVE-2021-26739	SQL Injection vulnerability in pay.php in millken doyocms 2.3, allows attackers to execute arbitrary code, via the attribute parameter.	9.8	More Details
CVE-2021-26740	Arbitrary file upload vulnerability sysupload.php in millken doyocms 2.3 allows attackers to execute arbitrary code.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20136	ManageEngine Log360 Builds < 5235 are affected by an improper access control vulnerability allowing database configuration overwrite. An unauthenticated remote attacker can send a specially crafted message to Log360 to change its backend database to an attacker-controlled database and to force Log360 to restart. An attacker can leverage this vulnerability to achieve remote code execution by replacing files executed by Log360 on startup.	9.8	More Details
CVE-2021-36560	Phone Shop Sales Managements System using PHP with Source Code 1.0 is vulnerable to authentication bypass which leads to account takeover of the admin.	9.8	More Details
CVE-2021-36794	In Siren Investigate before 11.1.4, when enabling the cluster feature of the Siren Alert application, TLS verifications are disabled globally in the Siren Investigate main process.	9.8	More Details
CVE-2020-18440	Buffer overflow vulnerability in framework/init.php in qinggan phpok 5.1, allows attackers to execute arbitrary code.	9.8	More Details
CVE-2020-23685	SQL Injection vulnerability in 188Jianzhan v2.1.0, allows attackers to execute arbitrary code and gain escalated privileges, via the username parameter to login.php.	9.8	More Details
CVE-2021-41646	Remote Code Execution (RCE) vulnerability exists in Sourcecodester Online Reviewer System 1.0 by uploading a maliciously crafted PHP file that bypasses the image upload filters..	9.8	More Details
CVE-2021-43267	An issue was discovered in net/tipc/crypto.c in the Linux kernel before 5.14.16. The Transparent Inter-Process Communication (TIPC) functionality allows remote attackers to exploit insufficient validation of user-supplied sizes for the MSG_CRYPTO message type.	9.8	More Details
CVE-2021-41643	Remote Code Execution (RCE) vulnerability exists in Sourcecodester Church Management System 1.0 via the image upload field.	9.8	More Details
CVE-2021-36990	There is a vulnerability of tampering with the kernel in Huawei Smartphone.Successful exploitation of this vulnerability may escalate permissions.	9.8	More Details
CVE-2011-4574	PolarSSL versions prior to v1.1 use the HAVEGE random number generation algorithm. At its heart, this uses timing information based on the processor's high resolution timer (the RDTSC instruction). This instruction can be virtualized, and some virtual machine hosts have chosen to disable this instruction, returning 0s or predictable results.	9.8	More Details
CVE-2020-24932	An SQL Injection vulnerability exists in Sourcecodester Complaint Management System 1.0 via the cid parameter in complaint-details.php.	9.8	More Details
CVE-2021-41589	In Gradle Enterprise before 2021.3 (and Enterprise Build Cache Node before 10.0), there is potential cache poisoning and remote code execution when running the build cache node with its default configuration. This configuration allows anonymous access to the configuration user interface and anonymous write access to the build cache. If access control to the build cache is not changed from the default open configuration, a malicious actor with network access can populate the cache with manipulated entries that may execute malicious code as part of a build process. This applies to the build cache provided with Gradle Enterprise and the separate build cache node service if used. If access control to the user interface is not changed from the default open configuration, a malicious actor can undo build cache access control in order to populate the cache with manipulated entries that may execute malicious code as part of a build process. This does not apply to the build cache provided with Gradle Enterprise, but does apply to the separate build cache node service if used.	9.8	More Details
CVE-2020-21250	CSZ CMS v1.2.4 was discovered to contain an arbitrary file upload vulnerability in the component /core/MY_Security.php.	9.8	More Details
CVE-2021-22403	There is a vulnerability of hijacking unverified providers 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.	9.8	More Details
CVE-2021-41676	An SQL Injection vulnerabilty exists in the oretnom23 Pharmacy Point of Sale System 1.0 in the login function in actions.php.	9.8	More Details
CVE-2021-36986	There is a vulnerability of tampering with the kernel in Huawei Smartphone.Successful exploitation of this vulnerability may escalate permissions.	9.8	More Details
CVE-2021-36989	There is a Kernel crash vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may escalate permissions.	9.8	More Details
CVE-2021-22474	There is an Out-of-bounds memory access in Huawei Smartphone.Successful exploitation of this vulnerability may cause process exceptions.	9.8	More Details
CVE-2021-37002	There is a Memory out-of-bounds access vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause malicious code to be executed.	9.8	More Details
CVE-2021-36548	A remote code execution (RCE) vulnerability in the component /admin/index.php?id=themes&action=edit_template&filename=blog of Monstra v3.0.4 allows attackers to execute arbitrary commands via a crafted PHP file.	9.8	More Details
CVE-2020-22079	Stack-based buffer overflow in Tenda AC-10U AC1200 Router US_AC10UV1.0RTL_V15.03.06.48_multi_TDE01 allows remote attackers to execute arbitrary code via the timeZone parameter to goform/SetSysTimeCfg.	9.8	More Details
CVE-2021-3756	libmysofa is vulnerable to Heap-based Buffer Overflow	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36547	A remote code execution (RCE) vulnerability in the component /codebase/dir.php?type=filenew of Mara v7.5 allows attackers to execute arbitrary commands via a crafted PHP file.	9.8	More Details
CVE-2021-41674	An SQL Injection vulnerability exists in Sourcecodester E-Negosyo System 1.0 via the user_email parameter in /admin/login.php.	9.8	More Details
CVE-2020-23718	Cross site scripting (XSS) vulnerability in xujinliang zibbs 1.0, allows attackers to execute arbitrary code via the route parameter to index.php.	9.6	More Details
CVE-2020-6492	Use after free in ANGLE in Google Chrome prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-37981	Heap buffer overflow in Skia in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-23754	Cross Site Scripting (XSS) vulnerability in infusions/member_poll_panel/poll_admin.php in PHP-Fusion 9.03.50, allows attackers to execute arbitrary code, via the polls feature.	9.6	More Details
CVE-2020-23719	Cross site scripting (XSS) vulnerability in application/controllers/AdminController.php in xujinliang zibbs 1.0, allows attackers to execute arbitrary code via the bbsmeta parameter.	9.6	More Details
CVE-2020-18439	An issue was discoverered in in function edit_save_f in framework/admin/tpl_control.php in qinggan phpok 5.1, allows attackers to write arbitrary files or get a shell.	9.1	More Details
CVE-2020-25911	A XML External Entity (XXE) vulnerability was discovered in the modRestServiceRequest component in MODX CMS 2.7.3 which can lead to an information disclosure or denial of service (DOS).	9.1	More Details
CVE-2021-38948	IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 211402.	9.1	More Details
CVE-2020-26705	The parseXML function in Easy-XML 0.5.0 was discovered to have a XML External Entity (XXE) vulnerability which allows for an attacker to expose sensitive data or perform a denial of service (DOS) via a crafted external entity entered into the XML content as input.	9.1	More Details
CVE-2021-22436	There is a Logic Bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service integrity and availability.	9.1	More Details
CVE-2021-41194	FirstUseAuthenticator is a JupyterHub authenticator that helps new users set their password on their first login to JupyterHub. When JupyterHub is used with FirstUseAuthenticator, a vulnerability in versions prior to 1.0.0 allows unauthorized access to any user's account if `create_users=True` and the username is known or guessed. One may upgrade to version 1.0.0 or apply a patch manually to mitigate the vulnerability. For those who cannot upgrade, there is no complete workaround, but a partial mitigation exists. One can disable user creation with `c.FirstUseAuthenticator.create_users = False`, which will only allow login with fully normalized usernames for already existing users prior to jupyterhub-firstuserauthenticator 1.0.0. If any users have never logged in with their normalized username (i.e. lowercase), they will still be vulnerable until a patch or upgrade occurs.	9.1	More Details
CVE-2020-25912	A XML External Entity (XXE) vulnerability was discovered in symphony\lib\toolkit\class.xmlelement.php in Symphony 2.7.10 which can lead to an information disclosure or denial of service (DOS).	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2020-23686	Cross site request forgery (CSRF) vulnerability in AyaCMS 3.1.2 allows attackers to change an administrators password or other unspecified impacts.
CVE-2021-31624	Buffer Overflow vulnerability in Tenda AC9 V1.0 through V15.03.05.19(6318), and AC9 V3.0 V15.03.06.42_multi, allows attackers to execute arbitrary code via the urls
CVE-2021-36185	A improper neutralization of special elements used in an OS command ('OS Command Injection') in Fortinet FortiWLM version 8.6.1 and below allows attacker to execu via crafted HTTP requests.
CVE-2021-36184	A improper neutralization of Special Elements used in an SQL Command ('SQL Injection') in Fortinet FortiWLM version 8.6.1 and below allows attacker to disclosure de via crafted HTTP requests.
CVE-2021-31627	Buffer Overflow vulnerability in Tenda AC9 V1.0 through V15.03.05.19(6318), and AC9 V3.0 V15.03.06.42_multi, allows attackers to execute arbitrary code via the inde

CVE Number	Description
CVE-2021-29844	IBM Jazz Team Server products is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the enumeration or facilitating other attacks.
CVE-2021-22038	On Windows, the uninstaller binary copies itself to a fixed temporary location, which is then executed (the originally called uninstaller exits, so it does not block the insta location is not randomized and does not restrict access to Administrators only so a potential attacker could plant a binary to replace the copied binary right before it gets privileges (if the original uninstaller was executed as Administrator). The vulnerability only affects Windows installers.
CVE-2021-39179	DHIS 2 is an information system for data capture, management, validation, analytics and visualization. A SQL Injection vulnerability in the Tracker component in DHIS2 attackers to execute arbitrary SQL commands via unspecified vectors. This vulnerability affects the `/api/trackedEntityInstances` and `/api/trackedEntityInstances/query 2.34, 2.35, and 2.36. It also affects versions 2.32 and 2.33 which have reached _end of support_ - exceptional security updates have been added to the latest *end of s Versions 2.31 and older are unaffected. The system is vulnerable to attack only from users that are logged in to DHIS2, and there is no known way of exploiting the vuln as a DHIS2 user. The vulnerability is not exposed to a non-malicious user - the vulnerability requires a conscious attack to be exploited. A successful exploit of this vuln user to read, edit and delete data in the DHIS2 instance. There are no known exploits of the security vulnerabilities addressed by these patch releases. Security patche 2.32-EOS, 2.33-EOS, 2.34.7, 2.35.7, and 2.36.4. There is no straightforward known workaround for DHIS2 instances using the Tracker functionality other than upgradi of the patches in which this vulnerability has been fixed. For implementations which do NOT use Tracker functionality, it may be possible to block all network access to `/api/trackedEntityInstances`, and `/api/trackedEntityInstances/query` endpoints as a temporary workaround while waiting to upgrade.
CVE-2021-41645	Remote Code Execution (RCE) vulnerability exists in Sourcecodester Budget and Expense Tracker System 1.0 that allows a remote malicious user to inject arbitrary co
CVE-2021-40348	Spacewalk 2.10, and derivatives such as Uyuni 2021.08, allows code injection. rhn-config-satellite.pl doesn't sanitize the configuration filename used to append Spacev script is intended to be run by the tomcat user account with Sudo, according to the installation setup. This can lead to the ability of an attacker to use --option to append that eventually will be executed by the system. This is fixed in Uyuni spacewalk-admin 4.3.2-1.
CVE-2021-29888	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmi trusts. IBM X-Force ID: 207123.
CVE-2021-24717	The AutomatorWP WordPress plugin before 1.7.6 does not perform capability checks which allows users with Subscriber roles to enumerate automations, disclose title functions, or perform privilege escalation via Ajax actions.
CVE-2021-24809	The BP Better Messages WordPress plugin before 1.9.9.41 does not check for CSRF in multiple of its AJAX actions: bp_better_messages_leave_chat, bp_better_mess bp_messages_leave_thread, bp_messages_mute_thread, bp_messages_unmute_thread, bp_better_messages_add_user_to_thread, bp_better_messages_exclude_u attackers to make logged in users do unwanted actions
CVE-2021-27644	In Apache DolphinScheduler before 1.3.6 versions, authorized users can use SQL injection in the data source center. (Only applicable to MySQL data source with inter
CVE-2021-37915	An issue was discovered on the Grandstream HT801 Analog Telephone Adaptor before 1.0.29.8. From the limited configuration shell, it is possible to set the malicious result, after a reboot, the device downloads and executes malicious scripts from an attacker-defined host.
CVE-2021-37748	Multiple buffer overflows in the limited configuration shell (/sbin/gs_config) on Grandstream HT801 devices before 1.0.29 allow remote authenticated users to execute a manage_if setting, thus bypassing the intended restrictions of this shell and taking full control of the device. There are default weak credentials that can be used to auth
CVE-2021-3901	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF)
CVE-2021-37221	A file upload vulnerability exists in Sourcecodester Customer Relationship Management System 1.0 via the account update option & customer create option, which cou an arbitrary php file. .
CVE-2021-36186	A stack-based buffer overflow in Fortinet FortiWeb version 6.4.0, version 6.3.15 and below, 6.2.5 and below allows attacker to execute unauthorized code or commands
CVE-2021-37977	Use after free in Garbage Collection in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37985	Use after free in V8 in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who had convinced a user to allow for connection to debugger to potentially exp HTML page.
CVE-2018-6122	Type confusion in WebAssembly in Google Chrome prior to 66.0.3359.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30809	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 15, tvOS 15, watchOS 8, iOS 15 and iPadOS 15. Processing ma lead to arbitrary code execution.

CVE Number	Description
CVE-2021-37993	Use after free in PDF Accessibility in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37992	Out of bounds read in WebAudio in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30818	A type confusion issue was addressed with improved state handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, tvOS 15, iOS 15 and iPadOS 15, Safari 15, watcl web content may lead to arbitrary code execution.
CVE-2021-37988	Use after free in Profiles in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who convinced a user to engage in specific gestures to potentially exploit h page.
CVE-2021-37987	Use after free in Network APIs in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37986	Heap buffer overflow in Settings in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to engage with Dev Tools to potentially exploit heap corruption via a
CVE-2021-38847	S-Cart v6.4.1 and below was discovered to contain an arbitrary file upload vulnerability in the Editor module on the Admin panel. This vulnerability allows attackers to e IMG file.
CVE-2021-37984	Heap buffer overflow in PDFium in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37983	Use after free in Dev Tools in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37982	Use after free in Incognito in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5123	Insufficient data validation in waitid allowed an user to escape sandboxes on Linux.
CVE-2021-37979	heap buffer overflow in WebRTC in Google Chrome prior to 94.0.4606.81 allowed a remote attacker who convinced a user to browse to a malicious website to potentia crafted HTML page.
CVE-2021-37978	Heap buffer overflow in Blink in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-34781	A vulnerability in the processing of SSH connections for multi-instance deployments of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated service (DoS) condition on the affected device. This vulnerability is due to a lack of proper error handling when an SSH session fails to be established. An attacker coul a high rate of crafted SSH connections to the instance. A successful exploit could allow the attacker to cause resource exhaustion, which causes a DoS condition on th be manually reloaded to recover.
CVE-2021-34783	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software c remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS mess software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit coul affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability.
CVE-2021-34793	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mo remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segment operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allo address tables in adjacent devices, resulting in network disruption.
CVE-2021-40118	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an u trigger a denial of service (DoS) condition. This vulnerability is due to improper input validation when parsing HTTPS requests. An attacker could exploit this vulnerabilit request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.
CVE-2021-34792	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauth denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could e significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.

CVE Number	Description
CVE-2021-40117	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow ar cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker c sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS conditio
CVE-2021-40116	Multiple Cisco products are affected by a vulnerability in Snort rules that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition o is due to improper handling of the Block with Reset or Interactive Block with Reset actions if a rule is configured without proper constraints. An attacker could exploit thi packet to the affected device. A successful exploit could allow the attacker to cause through traffic to be dropped. Note: Only products with Snort3 configured and eithe Interactive Block with Reset actions configured are vulnerable. Products configured with Snort2 are not vulnerable.
CVE-2021-41238	Hangfire is an open source system to perform background job processing in a .NET or .NET Core applications. No Windows Service or separate process required. Das authorization filters to protect it from showing sensitive data to unauthorized users. By default when no custom authorization filters specified, `LocalRequestsOnlyAutho allow only local requests and prohibit all the remote requests to provide sensible, protected by default settings. However due to the recent changes, in version 1.7.25 n default, allowing remote requests to succeed. If you are using `UseHangfireDashboard` method with default `DashboardOptions.Authorization` property value, then you authorization filter is specified in the `DashboardOptions.Authorization` property, the you are not impacted. Patched versions (1.7.26) are available both on Nuget.org a repo. Default authorization rules now prohibit remote requests by default again by including the `LocalRequestsOnlyAuthorizationFilter` filter to the default settings. Plea order to mitigate the issue. For users who are unable to upgrade it is possible to mitigate the issue by using the `LocalRequestsOnlyAuthorizationFilter` explicitly when
CVE-2021-31849	SQL injection vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.7.100 allows a remote attacker logged into ePO as an administrator to inje database through the user management section of the DLP ePO extension.
CVE-2021-31848	Cross site scripting (XSS) vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.7.100 allows a remote attacker to highjack an active DLP ePO the logged in administrator to click on a carefully crafted link in the case management part of the DLP ePO extension.
CVE-2021-42694	An issue was discovered in the character definitions of the Unicode Specification through 14.0. The specification allows an adversary to produce source code identifiers homoglyphs that render visually identical to a target identifier. Adversaries can leverage this to inject code via adversarial identifier definitions in upstream software dep downstream software. NOTE: the Unicode Consortium offers the following alternative approach to presenting this concern. An issue is noted in the nature of internation that implement support for The Unicode Standard (all versions). Unless mitigated, an adversary could produce source code identifiers using homoglyph characters that distinct from a target identifier. In this way, an adversary could inject adversarial identifier definitions in upstream software that are not detected by human reviewers an downstream software. The Unicode Consortium has documented this class of security vulnerability in its document, Unicode Technical Report #36, Unicode Security C Consortium also provides guidance on mitigations for this class of issues in Unicode Technical Standard #39, Unicode Security Mechanisms.
CVE-2021-42574	An issue was discovered in the Bidirectional Algorithm in the Unicode Specification through 14.0. It permits the visual reordering of characters via control sequences, w that renders different logic than the logical ordering of tokens ingested by compilers and interpreters. Adversaries can leverage this to encode source code for compiler targeted vulnerabilities are introduced invisibly to human reviewers. NOTE: the Unicode Consortium offers the following alternative approach to presenting this concern international text that can affect applications that implement support for The Unicode Standard and the Unicode Bidirectional Algorithm (all versions). Due to text displa right and right-to-left characters, the visual order of tokens may be different from their logical order. Additionally, control characters needed to fully support the requirem obfuscate the logical order of tokens. Unless mitigated, an adversary could craft source code such that the ordering of tokens perceived by human reviewers does not compiler/interpreter/etc. The Unicode Consortium has documented this class of vulnerability in its document, Unicode Technical Report #36, Unicode Security Conside provides guidance on mitigations for this class of issues in Unicode Technical Standard #39, Unicode Security Mechanisms, and in Unicode Standard Annex #31, Unic Also, the BIDI specification allows applications to tailor the implementation in ways that can mitigate misleading visual reordering in program text; see HL4 in Unicode S Bidirectional Algorithm.
CVE-2021-39341	The OptinMonster WordPress plugin is vulnerable to sensitive information disclosure and unauthorized setting updates due to insufficient authorization validation via th in the ~/OMAPI/RestApi.php file that can used to exploit inject malicious web scripts on sites with the plugin installed. This affects versions up to, and including, 2.6.4.
CVE-2021-39333	The Hashthemes Demo Importer Plugin <= 1.1.1 for WordPress contained several AJAX functions which relied on a nonce which was visible to all logged-in users for a execute a function that truncated nearly all database tables and removed the contents of wp-content/uploads.
CVE-2011-4126	Race condition issues were found in Calibre at devices/linux_mount_helper.c allowing unprivileged users the ability to mount any device to anywhere.
CVE-2021-41187	DHIS 2 is an information system for data capture, management, validation, analytics and visualization. A SQL injection security vulnerability has been found in specific affects the API endpoints for /api/trackedEntityInstances and api/events in DHIS2. The system is vulnerable to attack only from users that are logged in to DHIS2, and t the vulnerability without first being logged in as a DHIS2 user. A successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the exploits of the security vulnerabilities addressed by these patch releases. However, we strongly recommend that all DHIS2 implementations using versions 2.32, 2.33, patches as soon as possible. There is no straightforward known workaround for DHIS2 instances using the Tracker functionality other than upgrading the affected DHIS which this vulnerability has been fixed. For implementations which do NOT use Tracker functionality, it may be possible to block all network access to POST to the /api endpoints as a temporary workaround while waiting to upgrade.
CVE-2021-37803	An SQL Injection vulnerability exists in Sourcecodester Online Covid Vaccination Scheduler System 1.0 via the username in lognin.php .
CVE-2021-34762	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to perfo affected device. The attacker would require valid device credentials. The vulnerability is due to insufficient input validation of the HTTPS URL by the web-based manag exploit this vulnerability by sending a crafted HTTPS request that contains directory traversal character sequences to an affected device. A successful exploit could allo arbitrary files on the device.
CVE-2021-41232	Thunderdome is an open source agile planning poker tool in the theme of Battling for points. In affected versions there is an LDAP injection vulnerability which affects i enabled. The provided username is not properly escaped. This issue has been patched in version 1.16.3. If users are unable to update they should disable the LDAP fe

CVE Number	Description
CVE-2020-36503	The Connections Business Directory WordPress plugin before 9.7 does not validate or sanitise some connections' fields, which could lead to a CSV injection issue
CVE-2020-7867	An improper input validation vulnerability in Helpu solution could allow a local attacker to arbitrary file creation and execution without click file transfer menu. It is possib because the viewer program receive the file from agent with privilege of administrator.
CVE-2021-30834	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.8 and iPadOS 14.8, tvOS 15, iOS 15 and iPadOS 15, watchOS 8, Security Processing a malicious audio file may result in unexpected application termination or arbitrary code execution.
CVE-2021-30821	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.0.1, Security Update 2021-007 Catalina, macOS application may be able to execute arbitrary code with kernel privileges.
CVE-2021-22451	A component of the HarmonyOS has a Integer Overflow or Wraparound vulnerability. Local attackers may exploit this vulnerability to cause memory overwriting.
CVE-2021-30824	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.0.1, Security Update 2021-007 Catalina, macO application may be able to execute arbitrary code with kernel privileges.
CVE-2021-22470	A component of the HarmonyOS has a Privileges Controls vulnerability. Local attackers may exploit this vulnerability to expand the Recording Trusted Domain.
CVE-2021-30840	This issue was addressed with improved checks. This issue is fixed in tvOS 15, watchOS 8, iOS 15 and iPadOS 15. Processing a maliciously crafted dfont file may lead
CVE-2021-1118	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where there is the potential to execute privileged operations by the guest OS disclosure, data tampering, escalation of privileges, and denial of service
CVE-2020-23546	IrfanView 4.54 allows attackers to cause a denial of service or possibly other unspecified impacts via a crafted XBM file, related to a "Data from Faulting Address is use subsequent Function Call starting at FORMATS!ReadMosaic+0x0000000000000981.
CVE-2021-22458	A component of the HarmonyOS has a Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability. Local attackers may exploit this vulnerab execution.
CVE-2020-23549	IrfanView 4.54 allows attackers to cause a denial of service or possibly other unspecified impacts via a crafted .cr2 file, related to a "Data from Faulting Address control FORMATS!GetPlugInInfo+0x00000000000047f6".
CVE-2021-41022	A improper privilege management in Fortinet FortiSIEM Windows Agent version 4.1.4 and below allows attacker to execute privileged code or commands via powershe
CVE-2021-30814	A memory corruption issue was addressed with improved input validation. This issue is fixed in tvOS 15, watchOS 8, iOS 15 and iPadOS 15. Processing a maliciously c code execution.
CVE-2021-22037	Under certain circumstances, when manipulating the Windows registry, InstallBuilder uses the reg.exe system command. The full path to the command is not enforced, search path until a binary can be identified. This makes the installer/uninstaller vulnerable to Path Interception by Search Order Hijacking, potentially allowing an attack command so it takes precedence over the system command. The vulnerability only affects Windows installers.
CVE-2021-36925	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve an arbitrary read or write operation Escalation of Privileges, Denial of Service, Code Execution, and Information Disclosure) via a crafted Device IO Control packet to a device.
CVE-2021-3440	HP Print and Scan Doctor, an application within the HP Smart App for Windows, is potentially vulnerable to local elevation of privilege.
CVE-2021-36999	There is a Buffer overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability by sending malicious images and inducing users to open the i execution.
CVE-2021-36922	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve unauthorized access to USB devic Service, Code Execution, and Information Disclosure) via a crafted Device IO Control packet to a device.

CVE Number	Description
CVE-2021-36923	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve unauthorized access to USB devic (leading to Escalation of Privileges, Denial of Service, Code Execution, and Information Disclosure) via a crafted Device IO Control packet to a device.
CVE-2021-3903	vim is vulnerable to Heap-based Buffer Overflow
CVE-2020-9897	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.2 and iPadOS 14.2, macOS Big Sur 11.0.1. Processing a maliciously code execution.
CVE-2021-3576	Execution with Unnecessary Privileges vulnerability in Bitdefender Endpoint Security Tools, Total Security allows a local attacker to elevate to 'NT AUTHORITY\System thread to perform actions on behalf of the client but within the limits of the client's security context. This issue affects: Bitdefender Endpoint Security Tools versions prio Security versions prior to 25.0.26.
CVE-2021-3579	Incorrect Default Permissions vulnerability in the bdservicehost.exe and Vulnerability.Scan.exe components as used in Bitdefender Endpoint Security Tools for Window attacker to elevate privileges to NT AUTHORITY\SYSTEM This issue affects: Bitdefender Endpoint Security Tools for Windows versions prior to 7.2.1.65. Bitdefender T 7.2.1.65.
CVE-2021-43057	An issue was discovered in the Linux kernel before 5.14.8. A use-after-free in selinux_ptrace_traceme (aka the SELinux handler for PTRACE_TRACEME) could be use memory corruption and escalate privileges, aka CID-a3727a8bac0a. This occurs because of an attempt to access the subjective credentials of another task.
CVE-2021-36924	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve a pool overflow (leading to Escalat and Code Execution) via a crafted Device IO Control packet to a device.
CVE-2021-25742	A security issue was discovered in ingress-nginx where a user that can create or update ingress objects can use the custom snippets feature to obtain all secrets in the
CVE-2020-7875	DEXT5 Upload 5.0.0.117 and earlier versions contain a vulnerability, which could allow remote attacker to download and execute remote file by setting the argument, v can be leveraged for code execution.
CVE-2021-37991	Race in V8 in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37254	In M-Files Web product with versions before 20.10.9524.1 and 20.10.9445.0, a remote attacker could use a flaw to obtain unauthenticated access to 3rd party compone
CVE-2021-37001	There is a Register tampering vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow the register value to be modified.
CVE-2021-22044	In Spring Cloud OpenFeign 3.0.0 to 3.0.4, 2.2.0.RELEASE to 2.2.9.RELEASE, and older unsupported versions, applications using type-level `@RequestMapping`anno can be involuntarily exposing endpoints corresponding to `@RequestMapping`-annotated interface methods.
CVE-2021-36995	There is an Unauthorized file access vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability by modifying soft links may tamper with the files re
CVE-2021-42697	Akka HTTP 10.1.x before 10.1.15 and 10.2.x before 10.2.7 can encounter stack exhaustion while parsing HTTP headers, which allows a remote attacker to conduct a D User-Agent header with deeply nested comments.
CVE-2021-41874	An unauthorized access vulnerabiitly exists in all versions of Portainer, which could let a malicious user obtain sensitive information. NOTE: Portainer has received no c no response after multiple attempts of contacting the original source.
CVE-2020-21574	Buffer overflow vulnerability in YotsuyaNight c-http v0.1.0, allows attackers to cause a denial of service via a long url request which is passed to the delimitedread funct
CVE-2020-21572	Buffer overflow vulnerability in function src_parser_trans_stage_1_2_3 trgil gilcc before commit 803969389ca9c06237075a7f8eeb1a19e6651759, allows attackers to ca
CVE-2021-27722	An issue was discovered in Nsasoft US LLC SpotAuditor 5.3.5. The program can be crashed by entering 300 bytes char data into the "Key" or "Name" field while regist

CVE Number	Description
CVE-2021-37842	metakv in Couchbase Server 7.0.0 uses Cleartext for Storage of Sensitive Information. Remote Cluster XDCR credentials can get leaked in debug logs. Config key tom Couchbase Server 7.0.0. This issue happens when a config key, which is being logged, has a tombstone purger time-stamp attached to it.
CVE-2021-42763	Couchbase Server before 6.6.3 and 7.x before 7.0.2 stores Sensitive Information in Cleartext. The issue occurs when the cluster manager forwards a HTTP request fro etc) to the specific service. In the backtrace, the Basic Auth Header included in the HTTP request, has the "@" user credentials of the node processing the UI request.
CVE-2021-36992	There is a Public key verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2021-3704	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow a Denial of Service on the device.
CVE-2021-27005	Clustered Data ONTAP versions 9.6 and higher prior to 9.6P16, 9.7P16, 9.8P7 and 9.9.1P3 are susceptible to a vulnerability which could allow a remote attacker to cau
CVE-2020-28702	A SQL injection vulnerability in TopicMapper.xml of PybbsCMS v5.2.1 allows attackers to access sensitive database information.
CVE-2021-42557	In Jeedom through 4.1.19, a bug allows a remote attacker to bypass API access and retrieve users credentials.
CVE-2021-25874	AVideo/YouPHPTube AVideo/YouPHPTube 10.0 and prior is affected by a SQL Injection SQL injection in the catName parameter which allows a remote unauthenticat information such as application passwords hashes.
CVE-2021-29737	IBM InfoSphere Data Flow Designer Engine (IBM InfoSphere Information Server 11.7) component has improper validation of the REST API server certificate. IBM X-F
CVE-2021-29875	IBM InfoSphere Information Server 11.7 could allow an attacker to obtain sensitive information due to a insecure third party domain access vulnerability. IBM X-Force ID
CVE-2018-25019	The LearnDash LMS WordPress plugin before 2.5.4 does not have any authorisation and validation of the file to be uploaded in the learndash_assignment_process_ini unauthenticated users to upload arbitrary files to the web server
CVE-2015-20067	The WP Attachment Export WordPress plugin before 0.2.4 does not have proper access controls, allowing unauthenticated users to download the XML data that holds on a Wordpress
CVE-2020-18438	Directory traversal vulnerability in qinggan phpok 5.1, allows attackers to disclose sensitive information, via the title parameter to admin.php.
CVE-2020-20657	Buffer overflow vulnerability in fcovatti libiec_iccp_mod v1.5, allows attackers to cause a denial of service via an unexpected packet while trying to connect.
CVE-2020-20658	Buffer overflow vulnerability in fcovatti libiec_iccp_mod v1.5, allows attackers to cause a denail of service when trying to calloc an unexpectiedly large space.
CVE-2021-20838	Office Server Document Converter V7.2MR4 and earlier and V7.1MR7 and earlier allows a remote unauthenticated attacker to conduct an XML External Entity (XXE) a (DoS) condition by processing a specially crafted XML document.
CVE-2021-3765	validator.js is vulnerable to Inefficient Regular Expression Complexity
CVE-2021-41746	SQL Injection vulnerability exists in all versions of Yonyou TurboCRM.via the orgcode parameter in changepswd.php. Attackers can use the vulnerabilities to obtain ser
CVE-2021-36993	There is a Memory leaks vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability.

CVE Number	Description
CVE-2021-43270	Datalust Seq.App.EmailPlus (aka seq-app-htmlemail) 3.1.0-dev-00148, 3.1.0-dev-00170, and 3.1.0-dev-00176 can use cleartext SMTP on port 25 in some cases where intended.
CVE-2021-36991	There is an Unauthorized file access vulnerability in Huawei Smartphone due to unstandardized path input.Successful exploitation of this vulnerability by creating malic unauthorized file access.
CVE-2021-22473	There is an Authentication vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2021-34580	In mymbCONNECT24, mbCONNECT24 <= 2.9.0 an unauthenticated user can enumerate valid backend users by checking what kind of response the server sends for
CVE-2021-41872	Skyworth Digital Technology Penguin Aurora Box 41502 has a denial of service vulnerability, which can be exploited by attackers to cause a denial of service.
CVE-2021-22485	There is a SSID vulnerability with Wi-Fi network connections in Huawei devices.Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2021-22483	There is a issue of IP address spoofing in Huawei Smartphone. Successful exploitation of this vulnerability may cause DoS.
CVE-2021-22101	Cloud Controller versions prior to 1.118.0 are vulnerable to unauthenticated denial of Service(DoS) vulnerability allowing unauthenticated attackers to cause denial of s with label_selectors on multiple V3 endpoints by generating an enormous SQL query.
CVE-2021-22481	There is a Verification errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2021-37807	An SQL Injection vulneraility exists in https://phpgurukul.com Online Shopping Portal 3.1 via the email parameter on the /check_availability.php endpoint that serves as email is already exist within the database.
CVE-2021-37129	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input paramet of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200, V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10S V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20.
CVE-2021-22472	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2021-41191	Roblox-Purchasing-Hub is an open source Roblox product purchasing hub. A security risk in versions 1.0.1 and prior allowed people who have someone's API URL to This issue is fixed in version 1.0.2. As a workaround, add `@require_apikey` in `BOT/lib/cogs/website.py` under the route for `/v1/products`.
CVE-2021-22401	There is a Remote DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability can affect service integrity.
CVE-2021-22402	There is a DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause DoS attacks.
CVE-2021-22405	There is a Configuration defects in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability.
CVE-2021-22406	There is an Uncaught Exception vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the app to exit unexpectedly.
CVE-2021-37130	There is a path traversal vulnerability in Huawei FusionCube 6.0.2.The vulnerability is due to that the software uses external input to construct a pathname that is intend located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a locat directory by a crafted filename.

CVE Number	Description
CVE-2021-29774	IBM Jazz Team Server products could allow an authenticated user to obtain elevated privileges under certain configurations. IBM X-Force ID: 203025.
CVE-2021-36985	There is a Code injection vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may exhaust system resources and cause the system to resta
CVE-2021-22487	There is an Out-of-bounds read vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service availability.
CVE-2021-36988	There is a Parameter verification issue in Huawei Smartphone.Successful exploitation of this vulnerability can affect service integrity.
CVE-2021-22488	There is an Unauthorized file access vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability by modifying soft links may tamper with the files re
CVE-2021-22486	There is a issue of Unstandardized field names in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2021-22491	There is an Input verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability.
CVE-2021-37980	Inappropriate implementation in Sandbox in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially bypass site isolation via Windows.
CVE-2021-36183	An improper authorization vulnerability [CWE-285] in FortiClient for Windows versions 7.0.1 and below and 6.4.2 and below may allow a local unprivileged attacker to e via the named pipe responsible for Forticlient updates.
CVE-2021-43266	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, exporting collections via PDF export could lead to code execution via shell metacharacters in a collection nam 20.10.4, 21.04.3, and 21.10.1, exporting collections via PDF export could cause code execution
CVE-2021-37127	There is a signature management vulnerability in some huawei products. An attacker can forge signature and bypass the signature check. During firmware update proc vulnerability can cause the forged system file overwrite the correct system file. Affected product versions include:iManager NetEco V600R010C00CP2001,V600R010C00CP2002,V600R010C00SPC100,V600R010C00SPC110,V600R010C00SPC120,V600R010C00SPC200,V600R010C00SPC210, NetEco 6000 V600R009C00SPC100,V600R009C00SPC110,V600R009C00SPC120,V600R009C00SPC190,V600R009C00SPC200,V600R009C00SPC201,V600R009C00SPC202
CVE-2021-41189	DSpace is an open source turnkey repository application. In version 7.0, any community or collection administrator can escalate their permission up to become system exists in 7.0 and does not impact 6.x or below. This issue is patched in version 7.1. As a workaround, users of 7.0 may temporarily disable the ability for community or c permissions or workflows settings.
CVE-2021-41675	A Remote Code Execution (RCE) vulnerabilty exists in Sourcecodester E-Negosyo System 1.0 in /admin/produts/controller.php via the doInsert function, which validate
CVE-2021-26610	The move_uploaded_file function in godomall5 does not perform an integrity check of extension or authority when user upload file. This vulnerability allows an attacker
CVE-2021-25877	AVideo/YouPHPTube 10.0 and prior is affected by Insecure file write. An administrator privileged user is able to write files on filesystem using flag and code variables ir
CVE-2021-41619	An issue was discovered in Gradle Enterprise before 2021.1.2. There is potential remote code execution via the application startup configuration. The installation config administrators) allows specifying arbitrary Java Virtual Machine startup options. Some of these options, such as -XX:OnOutOfMemoryError, allow specifying a comman abused to run arbitrary commands on the host, should an attacker gain administrative access to the application.
CVE-2021-22469	A component of the HarmonyOS has a Out-of-bounds Read vulnerability. Local attackers may exploit this vulnerability to cause kernel out-of-bounds read.
CVE-2021-1119	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can double-free a pointer, which may lead to denial of service. This condition, allowing an attacker to execute arbitrary code impacting integrity and availability.
CVE-2021-3823	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in the UpdateServer component of Bitdefender GravityZone allows an attack vulnerable instances. This issue affects: Bitdefender GravityZone versions prior to 3.3.8.249.

CVE Number	Description
CVE-2021-1120	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a string provided by the guest OS may not be properly null terminate ability to push content to the plugin through this vulnerability, which may lead to information disclosure, data tampering, unauthorized code execution, and denial of ser
CVE-2021-40114	Multiple Cisco products are affected by a vulnerability in the way the Snort detection engine processes ICMP traffic that could allow an unauthenticated, remote attacke condition on an affected device. The vulnerability is due to improper memory resource management while the Snort detection engine is processing ICMP packets. An a by sending a series of ICMP packets through an affected device. A successful exploit could allow the attacker to exhaust resources on the affected device, causing the
CVE-2021-37131	There is a CSV injection vulnerability in ManageOne, iManager NetEco and iManager NetEco 6000. An attacker with high privilege may exploit this vulnerability through files. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject CSV files to the target device.
CVE-2021-22278	A certificate validation vulnerability in PCM600 Update Manager allows attacker to get unwanted software packages to be installed on computer which has PCM600 ins
CVE-2021-29213	A potential local bypass of security restrictions vulnerability has been identified in HPE ProLiant DL20 Gen10, HPE ProLiant ML30 Gen10, and HPE ProLiant MicroSer ROMs prior to version 2.52. The vulnerability could be locally exploited to cause disclosure of sensitive information, denial of service (DoS), and/or compromise system
CVE-2021-34756	Multiple vulnerabilities in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with ro about these vulnerabilities, see the Details section of this advisory.
CVE-2021-34755	Multiple vulnerabilities in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with ro about these vulnerabilities, see the Details section of this advisory.
CVE-2021-3745	flatcore-cms is vulnerable to Unrestricted Upload of File with Dangerous Type
CVE-2021-25973	In Publify, 9.0.0.pre1 to 9.2.4 are vulnerable to Improper Access Control. “guest” role users can self-register even when the admin does not allow. This happens due to
CVE-2021-24742	The Logo Slider and Showcase WordPress plugin before 1.3.37 allows Editor users to update the plugin's settings via the rtWLSSettings AJAX action because it uses a capability check.
CVE-2021-37995	Inappropriate implementation in WebApp Installer in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially overlay and spoof the contents of the HTML page.
CVE-2021-20839	Office Server Document Converter V7.2MR4 and earlier and V7.1MR7 and earlier allows a remote unauthenticated attacker to conduct an XML External Entity (XXE) a (DoS) condition to the other servers by processing a specially crafted XML document.
CVE-2021-3900	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF)
CVE-2020-36504	The WP-Pro-Quiz WordPress plugin through 0.37 does not have CSRF check in place when deleting a quiz, which could allow an attacker to make a logged in admin c
CVE-2021-37124	There is a path traversal vulnerability in Huawei PC product. Because the product does not filter path with special characters,attackers can construct a file path with spe vulnerability. Successful exploitation could allow the attacker to transport a file to certain path.Affected product versions include:PC Smart Full Scene 11.1 versions PCI
CVE-2020-36505	The Delete All Comments Easily WordPress plugin through 1.3 is lacking Cross-Site Request Forgery (CSRF) checks, which could result in an unauthenticated attacke comments from the blog.
CVE-2020-16048	Out of bounds read in ANGLE allowed a remote attacker to obtain sensitive data via a crafted HTML page.
CVE-2021-24770	The Stylish Price List WordPress plugin before 6.9.1 does not perform capability checks in its spl_upload_ser_img AJAX action (available to authenticated users), whicl users, such as subscriber, to upload arbitrary images.
CVE-2020-25873	A directory traversal vulnerability in the component system/manager/class/web/database.php was discovered in Baijiacms V4 which allows attackers to arbitrarily delete parameter.

CVE Number	Description
CVE-2018-6125	Insufficient policy enforcement in USB in Google Chrome on Windows prior to 67.0.3396.62 allowed a remote attacker to obtain potentially sensitive information via a cı
CVE-2021-37122	There is a use-after-free (UAF) vulnerability in Huawei products. An attacker may craft specific packets to exploit this vulnerability. Successful exploitation may cause th versions include:CloudEngine 12800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 5800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 6 V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800;CloudEngine 7800 V200R005C10SPC800,V200R019C00SPC800.
CVE-2021-32595	Multiple uncontrolled resource consumption vulnerabilities in the web interface of FortiPortal before 6.0.6 may allow a single low-privileged user to induce a denial of se
CVE-2021-37994	Inappropriate implementation in iFrame Sandbox in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to bypass navigation restrictions via a crafted HTM
CVE-2021-3906	bookstack is vulnerable to Unrestricted Upload of File with Dangerous Type
CVE-2021-37989	Inappropriate implementation in Blink in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to abuse content security policy via a crafted HTML page.
CVE-2021-1115	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for private IOCTLs, where an attacker with local unpr NULL pointer dereference, which may lead to denial of service in a component beyond the vulnerable component.
CVE-2021-36756	CFEngine Enterprise 3.15.0 through 3.15.4 has Missing SSL Certificate Validation.
CVE-2021-29786	IBM Jazz Team Server products stores user credentials in clear text which can be read by an authenticated user. IBM X-Force ID: 203172.
CVE-2021-41973	In Apache MINA, a specifically crafted, malformed HTTP request may cause the HTTP Header decoder to loop indefinitely. The decoder assumed that the HTTP Head buffer and loops if there is more data than expected. Please update MINA to 2.1.5 or greater.
CVE-2020-10005	A resource exhaustion issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1. An attacker in a privileged network position ma service.
CVE-2021-30823	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Monterey 12.0.1, iOS 14.8 and iPadOS 14.8, tvOS 15, Safari 15, watchOS 8. An a position may be able to bypass HSTS.
CVE-2021-30813	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.0.1. A person with access to a host Mac may be able to bypass the Login W locked instance of macOS.
CVE-2021-1821	A logic issue was addressed with improved state management. This issue is fixed in watchOS 7.6, macOS Big Sur 11.5. Visiting a maliciously crafted webpage may lea
CVE-2021-22097	In Spring AMQP versions 2.2.0 - 2.2.18 and 2.3.0 - 2.3.10, the Spring AMQP Message object, in its toString() method, will deserialize a body for a message with conter object. It is possible to construct a malicious java.util.Dictionary object that can cause 100% CPU usage in the application if the toString() method is called.
CVE-2021-26107	An improper access control vulnerability [CWE-284] in FortiManager versions 6.4.4 and 6.4.5 may allow an authenticated attacker with a restricted user profile to modif VDOMs using VPN Manager.
CVE-2021-38356	The NextScripts: Social Networks Auto-Poster <= 4.3.20 WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the $_REQUEST['page'] parameter which inc/nxs_class_snap.php by supplying the appropriate value 'nxssnap-post' to load the page in $_GET['page'] along with malicious JavaScript in $_POST['page'].
CVE-2021-41310	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vu feature (/secure/admin/AssociatedProjectsForCustomField.jspa). The affected versions are before version 8.5.19, from version 8.6.0 before 8.13.11, and from version 8
CVE-2021-33611	Missing output sanitization in test sources in org.webjars.bowergithub.vaadin:vaadin-menu-bar versions 1.0.0 through 1.2.0 (Vaadin 14.0.0 through 14.4.4) allows remo JavaScript in browser by opening crafted URL

CVE Number	Description
CVE-2020-35249	Cross Site Scripting (XSS) vulnerability in ElkarBackup 1.3.3, allows attackers to execute arbitrary code via the name parameter to the add client feature.
CVE-2021-31862	SysAid 20.4.74 allows XSS via the KeepAlive.jsp stamp parameter without any authentication.
CVE-2021-25878	AVideo/YouPHPTube 10.0 and prior is affected by multiple reflected Cross Script Scripting vulnerabilities via the videoName parameter which allows a remote attacker cookies or perform actions as an administrator.
CVE-2021-25876	AVideo/YouPHPTube 10.0 and prior has multiple reflected Cross Script Scripting vulnerabilities via the u parameter which allows a remote attacker to steal administrato actions as an administrator.
CVE-2021-25875	AVideo/YouPHPTube AVideo/YouPHPTube 10.0 and prior has multiple reflected Cross Script Scripting vulnerabilities via the searchPhrase parameter which allows a r administrators' session cookies or perform actions as an administrator.
CVE-2021-24808	The BP Better Messages WordPress plugin before 1.9.9.41 sanitise (with sanitize_text_field) but does not escape the 'subject' parameter before outputting it back in an Cross-Site Scripting issue
CVE-2021-36176	Multiple uncontrolled resource consumption vulnerabilities in the web interface of FortiPortal before 6.0.6 may allow a single low-privileged user to induce a denial of se
CVE-2021-43058	An open redirect vulnerability exists in Replicated Classic versions prior to 2.53.1 that could lead to spoofing. To exploit this vulnerability, an attacker could send a link t convince the user to click the link, redirecting the user to an untrusted site.
CVE-2021-41728	Cross Site Scripting (XSS) vulnerability exists in Sourcecodester News247 CMS 1.0 via the search function in articles.
CVE-2020-22312	A cross-site scripting (XSS) vulnerability was discovered in the OJ/admin-tool /cal_scores.php function of HZNUOJ v1.0.
CVE-2021-36987	There is a issue that nodes in the linked list being freed for multiple times in Huawei Smartphone due to race conditions. Successful exploitation of this vulnerability can
CVE-2021-37808	SQL Injection vulnerabilities exist in https://phpgurukul.com News Portal Project 3.1 via the (1) category, (2) subcategory, (3) sucatdescription, and (4) username param (N) seconds delay respectively which mean it is vulnerable to MySQL Blind (Time Based). An attacker can use sqlmap to further the exploitation for extracting sensitive
CVE-2021-41186	Fluentd collects events from various data sources and writes them to files to help unify logging infrastructure. The parser_apache2 plugin in Fluentd v0.14.14 to v1.14.1 denial of service (ReDoS) vulnerability. A broken apache log with a certain pattern of string can spend too much time in a regular expression, resulting in the potential fo in version 1.14.2 There are two workarounds available. Either don't use parser_apache2 for parsing logs (which cannot guarantee generated by Apache), or put patche /etc/fluent/plugin directory (or any other directories specified by the environment variable `FLUENT_PLUGIN` or `--plugin` option of fluentd).
CVE-2021-37806	An SQL Injection vulnerability exists in https://phpgurukul.com Vehicle Parking Management System affected version 1.0. The system is vulnerable to time-based SQL Based on the SLEEP(N) function payload that will sleep for a number of seconds used on the (1) editid , (2) viewid, and (3) catename parameters, the server response respectively which mean it is vulnerable to MySQL Blind (Time Based). An attacker can use sqlmap to further the exploitation for extracting sensitive information from th
CVE-2021-36808	A local attacker could bypass the app password using a race condition in Sophos Secure Workspace for Android before version 9.7.3115.
CVE-2021-34754	Multiple vulnerabilities in the payload inspection for Ethernet Industrial Protocol (ENIP) traffic for Cisco Firepower Threat Defense (FTD) Software could allow an unauth configured rules for ENIP traffic. These vulnerabilities are due to incomplete processing during deep packet inspection for ENIP packets. An attacker could exploit these ENIP packet to the targeted interface. A successful exploit could allow the attacker to bypass configured access control and intrusion policies that should be activated fo
CVE-2021-22471	A component of the HarmonyOS has a NULL Pointer Dereference vulnerability. Local attackers may exploit this vulnerability to cause nearby process crash.
CVE-2021-22463	A component of the HarmonyOS has a Use After Free vulnerability . Local attackers may exploit this vulnerability to cause Kernel Information disclosure.
CVE-2021-22455	A component of the HarmonyOS has a Integer Overflow or Wraparound vulnerability. Local attackers may exploit this vulnerability to cause the memory which is not rel

CVE Number	Description
CVE-2021-37996	Insufficient validation of untrusted input Downloads in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to bypass navigation restrictions via a malicious
CVE-2021-30836	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.8 and iPadOS 14.8, tvOS 15, watchOS 8, iOS 15 and iPadOS 15. Pr file may disclose restricted memory.
CVE-2021-1123	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can deadlock, which may lead to denial of service.
CVE-2021-22450	A component of the HarmonyOS has a Incomplete Cleanup vulnerability. Local attackers may exploit this vulnerability to cause memory exhaustion.
CVE-2021-1122	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can dereference a NULL pointer, which may lead to denial of servic
CVE-2021-30833	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.0.1. Unpacking a maliciously crafted archive may allow an attacker to write
CVE-2021-43056	An issue was discovered in the Linux kernel for powerpc before 5.14.15. It allows a malicious KVM guest to crash the host, when the host is running on Power8, due to arch/powerpc/kvm/book3s_hv_rmhandlers.S implementation bug in the handling of the SRR1 register values.
CVE-2021-22465	A component of the HarmonyOS has a Heap-based Buffer Overflow vulnerability. Local attackers may exploit this vulnerability to cause Kernel System unavailable.
CVE-2021-22466	A component of the HarmonyOS has a Use After Free vulnerability. Local attackers may exploit this vulnerability to cause kernel crash.
CVE-2021-22456	A component of the HarmonyOS has a Data Processing Errors vulnerability. Local attackers may exploit this vulnerability to cause Kernel System unavailable.
CVE-2021-22467	A component of the HarmonyOS has a Improper Input Validation vulnerability. Local attackers may exploit this vulnerability to read at any address.
CVE-2021-1121	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager kernel driver, where a vGPU can cause resource starvation among other vGPUs hosted on denial of service.
CVE-2021-42917	Buffer overflow vulnerability in Kodi xbmc up to 19.0, allows attackers to cause a denial of service due to improper length of values passed to istream.
CVE-2021-1116	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a NULL pointer dereference in the kernel, created wit denial of service in the form of a system crash.
CVE-2021-27004	System Manager 9.x versions 9.7 and higher prior to 9.7P16, 9.8P7 and 9.9.1P2 are susceptible to a vulnerability which could allow a local attacker to discover plaintex
CVE-2021-37990	Inappropriate implementation in WebView in Google Chrome on Android prior to 95.0.4638.54 allowed a remote attacker to leak cross-origin data via a crafted app.
CVE-2021-22454	A component of the HarmonyOS has a External Control of System or Configuration Setting vulnerability. Local attackers may exploit this vulnerability to cause core dun
CVE-2021-22461	A component of the HarmonyOS has a Allocation of Resources Without Limits or Throttling vulnerability. Local attackers may exploit this vulnerability to cause nearby p
CVE-2021-22459	A component of the HarmonyOS has a NULL Pointer Dereference vulnerability. Local attackers may exploit this vulnerability to cause System functions which are unav

CVE Number	Description
CVE-2021-22460	A component of the HarmonyOS has a Insufficient Verification of Data Authenticity vulnerability. Local attackers may exploit this vulnerability to bypass the control mecl
CVE-2020-29629	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1. A malicious application may be able to read restricte
CVE-2021-22452	A component of the HarmonyOS has a Improper Input Validation vulnerability. Local attackers may exploit this vulnerability to read at any address.
CVE-2021-30808	This issue was addressed with improved checks. This issue is fixed in tvOS 15, watchOS 8, iOS 15 and iPadOS 15. A malicious application may be able to modify prot
CVE-2021-41023	A unprotected storage of credentials in Fortinet FortiSIEM Windows Agent version 4.1.4 and below allows an authenticated user to disclosure agent password due to pl
CVE-2021-38379	The Hub in CFEngine Enterprise 3.6.7 through 3.18.0 has Insecure Permissions that allow local Information Disclosure.
CVE-2020-25881	A vulnerability was discovered in the filename parameter in pathindex.php?r=cms-backend/attachment/delete&sub=&filename=../../../../111.txt&filetype=image/jpeg of th vulnerability allows for an attacker to perform a directory traversal via a crafted .txt file.
CVE-2021-30817	A permissions issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.5. A malicious application may be able to access data about the a Sharing with.
CVE-2021-22462	A component of the HarmonyOS has a NULL Pointer Dereference vulnerability. Local attackers may exploit this vulnerability to cause kernel crash.
CVE-2021-29868	IBM i2 iBase 8.9.13 and 9.0.0 could allow a local attacker to obtain sensitive information due to insufficient session expiration. IBM X-Force ID: 206213.
CVE-2020-21573	An issue was discoverered in in abhijitnathwani image-processing v0.1.0, allows local attackers to cause a denial of service via a crafted image file.
CVE-2021-30831	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 15, watchOS 8, iOS 15 and iPadOS 15. Processing a maliciously craft process memory.
CVE-2021-29713	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the leading to credentials disclosure within a trusted session.
CVE-2021-29771	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus alteri potentially leading to credentials disclosure within a trusted session.
CVE-2021-29673	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the leading to credentials disclosure within a trusted session. IBM X-Force ID: 199482.
CVE-2021-36551	TikiWiki v21.4 was discovered to contain a cross-site scripting (XSS) vulnerability in the component tiki-calendar.php. This vulnerability allows attackers to execute arbit crafted payload under the Add Event module.
CVE-2021-37805	A Stored Cross Site Scripting (XSS) vunerability exists in Sourcecodeste Vehicle Parking Management System affected version 1.0 is via the add-vehicle.php endpoint
CVE-2021-36550	TikiWiki v21.4 was discovered to contain a cross-site scripting (XSS) vulnerability in the component tiki-browse_categories.php. This vulnerability allows attackers to ex via a crafted payload under the Create category module.
CVE-2021-43265	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, certain tag syntax could be used for XSS, such as via a SCRIPT element.

CVE Number	Description
CVE-2021-29738	IBM InfoSphere Data Flow Designer (IBM InfoSphere Information Server 11.7) is vulnerable to server-side request forgery (SSRF). This may allow an authenticated at from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 201302.
CVE-2020-25422	A cross site scripting (XSS) vulnerability in menuedit.php of Mara CMS 7.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.
CVE-2020-27406	Cross Site Scripting (XSS) vulnerability in DynPG 4.9.1, allows authenticated attackers to execute arbitrary code via the groupname.
CVE-2021-24716	The Modern Events Calendar Lite WordPress plugin before 5.22.3 does not properly sanitize or escape values set by users with access to adjust settings withing wp-ad
CVE-2021-3904	grav is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CVE-2021-24723	The WP Reactions Lite WordPress plugin before 1.3.6 does not properly sanitize inputs within wp-admin pages, allowing users with sufficient access to inject XSS payl
CVE-2021-24685	The Flat Preloader WordPress plugin before 1.5.4 does not enforce nonce checks when saving its settings, as well as does not sanitise and escape them, which could admin change them with a Cross-Site Scripting payload (triggered either in the frontend or backend depending on the payload)
CVE-2021-24682	The Cool Tag Cloud WordPress plugin before 2.26 does not escape the style attribute of the cool_tag_cloud shortcode, which could allow users with a role as low as C Site Scripting attacks.
CVE-2015-20019	The Content text slider on post WordPress plugin before 6.9 does not sanitise and escape the Title and Message/Content settings, which could lead to Cross-Site Scrip
CVE-2021-3662	Certain HP Enterprise LaserJet and PageWide MFPs may be vulnerable to stored cross site scripting (XSS).
CVE-2021-35233	The HTTP TRACK & TRACE methods were enabled in Kiwi Syslog Server 9.7.1 and earlier. These methods are intended for diagnostic purposes only. If enabled, the v that use these methods by returning exact HTTP request that was received in the response to the client. This may lead to the disclosure of sensitive information such a appended by reverse proxies.
CVE-2021-24757	The Stylish Price List WordPress plugin before 6.9.0 does not perform capability checks in its spl_upload_ser_img AJAX action (available to both unauthenticated and a allow unauthenticated users to upload images.
CVE-2021-22475	There is an Improper permission management vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2021-36996	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause transmission of certain virtual information.
CVE-2021-20526	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploi information from the cookie. IBM X-Force ID: 198755.
CVE-2021-36997	There is a Low memory error in Huawei Smartphone due to the unlimited size of images to be parsed.Successful exploitation of this vulnerability may cause the Gallery
CVE-2021-36187	A uncontrolled resource consumption in Fortinet FortiWeb version 6.4.0, version 6.3.15 and below, 6.2.5 and below allows attacker to cause a denial of service for web requests
CVE-2021-22482	There is an Uninitialized variable vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause transmission of invalid data.
CVE-2021-33259	Several web interfaces in D-Link DIR-868LW 1.12b have no authentication requirements for access, allowing for attackers to obtain users' DNS query history.

CVE Number	Description
CVE-2021-41590	In Gradle Enterprise through 2021.3, probing of the server-side network environment can occur via an SMTP configuration test. The installation configuration user interf testing the configured SMTP server settings. This test function can be used to identify the listening TCP ports available to the server, revealing information about the int
CVE-2021-22407	There is a Configuration defects in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2021-22404	There is a Directory traversal vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2021-22047	In Spring Data REST versions 3.4.0 - 3.4.13, 3.5.0 - 3.5.5, and older unsupported versions, HTTP resources implemented by custom controllers using a configured bas request mapping are additionally exposed under URIs that can potentially be exposed for unauthorized access depending on the Spring Security configuration.
CVE-2021-22490	There is a Permission verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect the device performance.
CVE-2021-32951	WebAccess/NMS (Versions prior to v3.0.3_Build6299) has an improper authentication vulnerability, which may allow unauthorized users to view resources monitored a WebAccess/NMS, as well as IP addresses and names of all the devices managed via WebAccess/NMS.
CVE-2021-35235	The ASP.NET debug feature is enabled by default in Kiwi Syslog Server 9.7.2 and previous versions. ASP.NET allows remote debugging of web applications, if configu ASP.NET to compile applications with extra information. The information enables a debugger to closely monitor and control the execution of an application. If an attacke debugging session, this is likely to disclose sensitive information about the web application and supporting infrastructure that may be valuable in targeting SWI with mal
CVE-2021-36998	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to read an array that is out of boun
CVE-2021-40125	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defen authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacke IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messa successful exploit could allow the attacker to trigger a reload of the device.
CVE-2021-34787	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to us could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access contr bypass security protections, and send network traffic to unauthorized hosts.
CVE-2021-25219	In BIND 9.3.0 -> 9.11.35, 9.12.0 -> 9.16.21, and versions 9.9.3-S1 -> 9.11.35-S1 and 9.16.8-S1 -> 9.16.21-S1 of BIND Supported Preview Edition, as well as release v 9.17 development branch, exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The w designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing.
CVE-2021-34794	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit th SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMF retrieve information from the device. The attacker would need valid credentials to perform the SNMP query.
CVE-2021-33593	Whale browser for iOS before 1.14.0 has an inconsistent user interface issue that allows an attacker to obfuscate the address bar which may lead to address bar spoof
CVE-2021-35237	A missing HTTP header (X-Frame-Options) in Kiwi Syslog Server has left customers vulnerable to click jacking. Clickjacking is an attack that occurs when an attacker u to trick a user into clicking on an actionable item, such as a button or link, to another server in which they have an identical webpage. The attacker essentially hijacks th original server and sends them to the other server. This is an attack on both the user and the server.
CVE-2020-25872	A vulnerability exists within the FileManagerController.php function in FrogCMS 0.9.5 which allows an attacker to perform a directory traversal attack via a GET request
CVE-2021-24624	The MP3 Audio Player for Music, Radio & Podcast by Sonaar WordPress plugin before 2.4.2 does not properly sanitize or escape data in some of its Playlist settings, a perform Cross-Site Scripting attacks
CVE-2021-34764	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an attacker to execute a cross-site redirect attack. For more information about these vulnerabilities, see the Details section of this advisory.
CVE-2021-34763	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an attacker to execute a cross-site redirect attack. For more information about these vulnerabilities, see the Details section of this advisory.
CVE-2021-24715	The WP Sitemap Page WordPress plugin before 1.7.0 does not properly sanitise and escape some of its settings, which could allow high privilege users to perform Cro the unfiltered_html capability is disallowed.

CVE Number	Description
CVE-2021-24539	The Coming Soon, Under Construction & Maintenance Mode By Dazzler WordPress plugin before 1.6.7 does not sanitise or escape its description setting when outputt Coming Soon mode is enabled, even when the unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue
CVE-2021-24722	The Restaurant Menu by MotoPress WordPress plugin before 2.4.2 does not properly sanitize or escape inputs when creating new menu items, which could allow high Scripting attacks even when the unfiltered_html capability is disallowed
CVE-2021-39346	The Google Maps Easy WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found i ~/modules/marker_groups/views/tpl/mgrEditMarkerGroup.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.
CVE-2021-24789	The Flat Preloader WordPress plugin before 1.5.5 does not escape some of its settings when outputting them in attribute in the frontend, which could allow high privileg Scripting attacks even when the unfiltered_html is disallowed
CVE-2021-24793	The WPeMatico RSS Feed Fetcher WordPress plugin before 2.6.12 does not escape the Feed URL added to a campaign before outputting it in an attribute, allowing hi Site Scripting attacks even when the unfiltered_html capability is disallowed.
CVE-2021-3441	A potential security vulnerability has been identified for the HP OfficeJet 7110 Wide Format ePrinter that enables Cross-Site Scripting (XSS).
CVE-2021-24794	The Connections Business Directory WordPress plugin before 10.4.3 does not escape the Address settings when creating an Entry, which could allow high privilege us when the unfiltered_html capability is disallowed.
CVE-2021-39340	The Notification WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/ which made it possible for attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 7.2.4. This affects multi-site installatio for administrators, and sites where unfiltered_html is disabled.
CVE-2021-24813	The Events Made Easy WordPress plugin before 2.2.24 does not sanitise and escape Custom Field Names, allowing high privilege users to perform Cross-Site Scriptir unfiltered_html capability is disallowed
CVE-2021-24773	The WordPress Download Manager WordPress plugin before 3.2.16 does not escape some of the Download settings when outputting them, allowing high privilege use the unfiltered_html capability is disallowed
CVE-2021-34790	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more i vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming.
CVE-2021-34791	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more i vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming.
CVE-2021-1117	Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where an attacker through specific configuration and with local u cause improper input validation, which may lead to denial of service.
CVE-2021-22563	Invalid JPEG XL images using libjxl can cause an out of bounds access on a std::vector<std::vector<T>> when rendering splines. The OOB read access can either lea based on other process memory. It is recommended to upgrade past 0.6.0 or patch with https://github.com/libjxl/libjxl/pull/757
CVE-2021-22564	For certain valid JPEG XL images with a size slightly larger than an integer number of groups (256x256 pixels) when processing the groups out of order the decoder ca image pixels from an image buffer in the heap to another. This copy can occur when processing the right or bottom edges of the image, but only when groups are proce processed out of order in multi-threaded decoding environments with heavy thread load but also with images that contain the groups in an arbitrary order in the file. It is or patch with https://github.com/libjxl/libjxl/pull/775
CVE-2021-34761	A vulnerability in Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to overwrite or append arbitrary data to system files using must have administrative credentials on the device. This vulnerability is due to incomplete validation of user input for a specific CLI command. An attacker could exploit the device with administrative privileges and issuing a CLI command with crafted user parameters. A successful exploit could allow the attacker to overwrite or append root-level privileges.
CVE-2021-24781	The Image Source Control WordPress plugin before 2.3.1 allows users with a role as low as Contributor to change arbitrary post meta fields of arbitrary posts (even tho
CVE-2021-36172	An improper restriction of XML external entity reference vulnerability in the parser of XML responses of FortiPortal before 6.0.6 may allow an attacker who controls the by FortiPortal to trigger a denial of service or read arbitrary files from the underlying file system by means of specifically crafted XML documents.

CVE Number	Description
CVE-2021-41313	Affected versions of Atlassian Jira Server and Data Center allow authenticated but non-admin remote attackers to edit email batch configurations via an Improper Autho /secure/admin/ConfigureBatching!default.jspa endpoint. The affected versions are before version 8.20.7.
CVE-2021-42568	Sonatype Nexus Repository Manager 3.x through 3.35.0 allows attackers to access the SSL Certificates Loading function via a low-privileged account.
CVE-2021-22096	In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of
CVE-2015-10001	The WP-Stats WordPress plugin before 2.52 does not have CSRF check when saving its settings, and did not escape some of them when outputting them, allowing att privilege users change them and set Cross-Site Scripting payloads
CVE-2021-36174	A memory allocation with excessive size value vulnerability in the license verification function of FortiPortal before 6.0.6 may allow an attacker to perform a denial of se license blobs.
CVE-2020-15935	A cleartext storage of sensitive information in GUI in FortiADC versions 5.4.3 and below, 6.0.0 and below may allow a remote authenticated attacker to retrieve some s LDAP passwords and RADIUS shared secret by deobfuscating the passwords entry fields.
CVE-2021-24572	The Accept Donations with PayPal WordPress plugin before 1.3.1 provides a function to create donation buttons which are internally stored as posts. The deletion of a there is no control to check if the deleted post was a button post. As a result, an attacker could make logged in admins delete arbitrary posts
CVE-2021-24799	The Far Future Expiry Header WordPress plugin before 1.5 does not have CSRF check when saving its settings, which could allow attackers to make a logged in admi
CVE-2021-24570	The Accept Donations with PayPal WordPress plugin before 1.3.1 offers a function to create donation buttons, which internally are posts. The process to create a new attacker could use this to make an authenticated admin create a new button. Furthermore, one of the Button field is not escaped before being output in an attribute whe Stored Cross-Site Scripting issue as well.
CVE-2020-12814	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiAnalyzer version 6.0.6 and below, version 6.4.4 allows attacker to e commands via specifically crafted requests to the web GUI.
CVE-2020-15940	An improper neutralization of input vulnerability [CWE-79] in FortiClientEMS versions 6.4.1 and below and 6.2.9 and below may allow a remote authenticated attacker t name parameter of various sections of the server.
CVE-2021-36994	There is a issue that trustlist strings being repeatedly inserted into the linked list in Huawei Smartphone due to race conditions. Successful exploitation of this vulnerabil managing the system trustlist.
CVE-2021-41019	An improper validation of certificate with host mismatch [CWE-297] vulnerability in FortiOS versions 6.4.6 and below may allow the connection to a malicious LDAP ser disclosure of sensitive information, such as AD credentials.
CVE-2021-22468	A component of the HarmonyOS has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability. Local attackers may exploit this vulnerability to cause
CVE-2021-22453	A component of the HarmonyOS has a Improper Input Validation vulnerability. Local attackers may exploit this vulnerability to cause nearby process crash.
CVE-2021-22457	A component of the HarmonyOS has a Improper Input Validation vulnerability. Local attackers may exploit this vulnerability to cause out-of-bounds write.
CVE-2021-43264	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, adjusting the path component for the page help file allows attackers to bypass the intended access control for replaces the - character with the / character.
CVE-2021-22464	A component of the HarmonyOS has a Out-of-bounds Read vulnerability. Local attackers may exploit this vulnerability to cause system Soft Restart.
CVE-2021-42754	An improper control of generation of code vulnerability [CWE-94] in FortiClientMacOS versions 7.0.0 and below and 6.4.5 and below may allow an authenticated attack without the user permission via the malicious dylib file.

CVE Number	Description
CVE-2021-36181	A concurrent execution using shared resource with improper Synchronization vulnerability ('Race Condition') in the customer database interface of FortiPortal before 6.(privilege user to bring the underlying database data into an inconsistent state via specific coordination of web requests.
CVE-2021-35236	The Secure flag is not set in the SSL Cookie of Kiwi Syslog Server 9.7.2 and previous versions. The Secure attribute tells the browser to only send the cookie if the req channel such as HTTPS. This will help protect the cookie from being passed over unencrypted requests. If the application can be accessed over both HTTP, there is a clear text.
CVE-2021-30816	The issue was addressed with improved permissions logic. This issue is fixed in iOS 15 and iPadOS 15. An attacker with physical access to a device may be able to se
CVE-2018-14640	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none
CVE-2018-10909	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that none
CVE-2019-13776	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that some publications have used this number when they meant to use CVE-2019-13376
CVE-2018-1105	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that none
CVE-2021-37960	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that none
CVE-2021-41748	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-41874. Reason: This candidate is a duplicate of CVE-2021-41874. Notes: All CV 41874 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage
CVE-2018-6044	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2018-16064. Reason: This candidate is a reservation duplicate of CVE-2018-16064. N CVE-2018-16064 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage
CVE-2018-6058	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2017-11215. Reason: This candidate is a reservation duplicate of CVE-2017-11215. N CVE-2017-11215 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage
CVE-2018-6059	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2017-11225. Reason: This candidate is a reservation duplicate of CVE-2017-11225. N CVE-2017-11225 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage
CVE-2019-5863	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that none
CVE-2021-27723	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that none
CVE-2021-30631	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that none