SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 26 May 2021

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-33509	Plone through 5.2.4 allows remote authenticated managers to perform disk I/O via crafted keyword arguments to the ReStructuredText transform in a Python script.	9.9	More Details
CVE-2017-17674	BMC Remedy Mid Tier 9.1SP3 is affected by remote and local file inclusion. Due to the lack of restrictions on what can be targeted, the system can be vulnerable to attacks such as system fingerprinting, internal port scanning, Server Side Request Forgery (SSRF), or remote code execution (RCE).	9.8	More Details
CVE-2020-25409	Projectsworlds College Management System Php 1.0 is vulnerable to SQL injection issues over multiple parameters.	9.8	More Details
CVE-2021-33204	In the pg_partman (aka PG Partition Manager) extension before 4.5.1 for PostgreSQL, arbitrary code execution can be achieved via SECURITY DEFINER functions because an explicit search_path is not set.	9.8	More Details
CVE-2020-28902	Command Injection in Nagios Fusion 4.1.8 and earlier allows Privilege Escalation from apache to root in cmd_subsys.php.	9.8	More Details
CVE-2020-28904	Execution with Unnecessary Privileges in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation as nagios via installation of a malicious component containing PHP code.	9.8	More Details
CVE-2020-28907	Incorrect SSL certificate validation in Nagios Fusion 4.1.8 and earlier allows for Escalation of Privileges or Code Execution as root via vectors related to download of an untrusted update package in upgrade_to_latest.sh.	9.8	More Details
CVE-2020-28908	Command Injection in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation to nagios.	9.8	More Details
CVE-2020-28910	Creation of a Temporary Directory with Insecure Permissions in Nagios XI 5.7.5 and earlier allows for Privilege Escalation via creation of symlinks, which are mishandled in getprofile.sh.	9.8	More Details
CVE-2021-32075	Re-Logic Terraria before 1.4.2.3 performs Insecure Deserialization.	9.8	More Details
CVE-2021-20426	IBM Security Guardium 11.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 196313.	9.8	More Details
CVE-2019-12348	An issue was discovered in zzcms 2019. SQL Injection exists in user/ztconfig.php via the daohang or img POST parameter.	9.8	More Details
CVE-2021-29300	The @ronomon/opened library before 1.5.2 is vulnerable to a command injection vulnerability which would allow a remote attacker to execute commands on the system if the library was used with untrusted input.	9.8	More Details
CVE-2021-30188	CODESYS V2 runtime system SP before 2.4.7.55 has a Stack-based Buffer Overflow.	9.8	More Details
CVE-2021-30189	CODESYS V2 Web-Server before 1.1.9.20 has a Stack-based Buffer Overflow.	9.8	More Details
CVE-2021-30190	CODESYS V2 Web-Server before 1.1.9.20 has Improper Access Control.	9.8	More Details
CVE-2021-30192	CODESYS V2 Web-Server before 1.1.9.20 has an Improperly Implemented Security Check.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30193	CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Write.	9.8	More Details
CVE-2021-25944	Prototype pollution vulnerability in 'deep-defaults' versions 1.0.0 through 1.0.5 allows attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2021-25946	Prototype pollution vulnerability in `nconf-toml` versions 0.0.1 through 0.0.2 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2021-33574	The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or possibly unspecified other impact.	9.8	More Details
CVE-2020-28900	Insufficient Verification of Data Authenticity in Nagios Fusion 4.1.8 and earlier and Nagios XI 5.7.5 and earlier allows for Escalation of Privileges or Code Execution as root via vectors related to an untrusted update package to upgrade_to_latest.sh.	9.8	More Details
CVE-2020-28901	Command Injection in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation or Code Execution as root via vectors related to corrupt component installation in cmd_subsys.php.	9.8	More Details
CVE-2021-33575	The Pixar ruby-jss gem before 1.6.0 allows remote attackers to execute arbitrary code because of the Plist gem's documented behavior of using Marshal.load during XML document processing.	9.8	More Details
CVE-2021-31474	This vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Network Performance Monitor 2020.2.1. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SolarWinds.Serialization library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-12213.	9.8	More Details
CVE-2021-20720	SQL injection vulnerability in the KonaWiki2 versions prior to 2.2.4 allows remote attackers to execute arbitrary SQL commands and to obtain/alter the information stored in the database via unspecified vectors.	9.8	More Details
CVE-2020-36329	A flaw was found in libwebp in versions before 1.0.1. A use-after-free was found due to a thread being killed too early. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	9.8	More Details
CVE-2020-36328	A flaw was found in libwebp in versions before 1.0.1. A heap-based buffer overflow in function WebPDecodeRGBInto is possible due to an invalid check for buffer size. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	9.8	More Details
CVE-2018-25014	A use of uninitialized value was found in libwebp in versions before 1.0.1 in ReadSymbol().	9.8	More Details
CVE-2021-20721	KonaWiki2 versions prior to 2.2.4 allows a remote attacker to upload arbitrary files via unspecified vectors. If the file contains PHP scripts, arbitrary code may be executed.	9.8	More Details
CVE-2018-25011	A heap-based buffer overflow was found in libwebp in versions before 1.0.1 in PutLE16().	9.8	More Details
CVE-2021-27459	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an attacker could utilize to execute arbitrary code.	9.8	More Details
CVE-2020-12061	An issue was discovered in Nitrokey FIDO U2F firmware through 1.1. Communication between the microcontroller and the secure element transmits credentials in plain. This allows an adversary to eavesdrop the communication and derive the secrets stored in the microcontroller. As a result, the attacker is able to arbitrarily manipulate the firmware of the microcontroller.	9.8	More Details
CVE-2021-32630	Admidio is a free, open source user management system for websites of organizations and groups. In Admidio before version 4.0.4, there is an authenticated RCE via .phar file upload. A php web shell can be uploaded via the Documents & Files upload feature. Someone with upload permissions could rename the php shell with a .phar extension, visit the file, triggering the payload for a reverse/bind shell. This can be mitigated by excluding a .phar file extension to be uploaded (like you did with .php .phtml .php5 etc). The vulnerability is patched in version 4.0.4.	9.6	More Details
CVE-2020-36364	An issue was discovered in Smartstore (aka SmartStoreNET) before 4.1.0. Administration/Controllers/ImportController.cs allows path traversal (for copy and delete actions) in the ImportController.Create method via a TempFileName field.	9.1	More Details
CVE-2021-21658	Jenkins Nuget Plugin 1.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	9.1	More Details
CVE-2021-30194	CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Read.	9.1	More Details
CVE-2021-21001	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges.	9.1	More Details
CVE-2018-25009	A heap-based buffer overflow was found in libwebp in versions before 1.0.1 in GetLE16().	9.1	More Details
CVE-2021-33497	Dutchcoders transfer.sh before 1.2.4 allows Directory Traversal for deleting files.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20907	MetInfo 7.0 beta is affected by a file modification vulnerability. Attackers can delete and modify ini files in app/system/language/admin/language_general.class.php and app/system/include/function/file.func.php.	9.1	More Details
CVE-2018-25010	A heap-based buffer overflow was found in libwebp in versions before 1.0.1 in ApplyFilter().	9.1	More Details
CVE-2018-25012	A heap-based buffer overflow was found in libwebp in versions before 1.0.1 in GetLE24().	9.1	More Details
CVE-2018-25013	A heap-based buffer overflow was found in libwebp in versions before 1.0.1 in ShiftBytes().	9.1	More Details
CVE-2020-36330	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function ChunkVerifyAndAssign. The highest threat from this vulnerability is to data confidentiality and to the service availability.	9.1	More Details
CVE-2020-36331	A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function ChunkAssignData. The highest threat from this vulnerability is to data confidentiality and to the service availability.	9.1	More Details
CVE-2021-30108	Feehi CMS 2.1.1 is affected by a Server-side request forgery (SSRF) vulnerability. When the user modifies the HTTP Referer header to any url, the server can make a request to it.	9.1	More Details
CVE-2020-13601	Possible read out of bounds in dns read. Zephyr versions >= 1.14.2, >= 2.3.0 contain Out-of-bounds Read (CWE-125). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-mm57-9hqw-qh44	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2021-1531	A vulnerability in the web UI of Cisco Modeling Labs could allow an authenticated, remote attacker to execute arbitrary commands with the privileges of the web applica underlying operating system of an affected Cisco Modeling Labs server. This vulnerability is due to insufficient validation of user-supplied input to the web UI. An attack vulnerability by sending a crafted HTTP request to an affected server. A successful exploit could allow the attacker to execute arbitrary commands with the privileges of virl2, on the underlying operating system of the affected server. To exploit this vulnerability, the attacker must have valid user credentials on the web UI.
CVE-2020-28905	Improper Input Validation in Nagios Fusion 4.1.8 and earlier allows an authenticated attacker to execute remote code via table pagination.
CVE-2021-33514	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 bef GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510T and MS510TXUP before 1.0.2.3.
CVE-2021-28112	Draeger X-Dock Firmware before 03.00.13 has Active Debug Code on a debug port, leading to remote code execution by an authenticated attacker.
CVE-2021-1487	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Evolved Programmable Network (EPN) Manager could allow an authenticated execute arbitrary commands on an affected system. The vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An exploit this vulnerability by sending crafted HTTP requests to the interface. A successful exploit could allow the attacker to execute arbitrary commands on the underlyi (OS) with the permissions of a special non-root user. In this way, an attacker could take control of the affected system, which would allow them to obtain and alter sensi attacker could also affect the devices that are managed by the affected system by pushing arbitrary configuration files, retrieving device credentials and confidential info ultimately undermining the stability of the devices, causing a denial of service (DoS) condition.
CVE-2021-31475	This vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Orion Job Scheduler 2020.2.1 HF 2. Authentication is require vulnerability. The specific flaw exists within the JobRouterService WCF service. The issue is due to the WCF service configuration, which allows a critical resource to b unprivileged users. An attacker can leverage this vulnerability to execute code in the context of an administrator. Was ZDI-CAN-12007.
CVE-2021-25931	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-founda meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to CSRF, due to no CSRF protection at `/opennms/admin/userGroupView/users flaw allows assigning `ROLE_ADMIN` security role to a normal user. Using this flaw, an attacker can trick the admin user to assign administrator privileges to a normal to click upon an attacker-controlled website.
CVE-2021-31439	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Synology DiskStation Manager. Authentication is not required t vulnerablity. The specific flaw exists within the processing of DSI structures in Netatalk. The issue results from the lack of proper validation of the length of user-supplie copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12326.
CVE-2021-29686	IBM Security Identity Manager 7.0.2 could allow an authenticated user to bypass security and perform actions that they should not have access to. IBM X-Force ID: 200
CVE-2021-33525	EyesOfNetwork eonweb through 5.3-11 allows Remote Command Execution (by authenticated users) via shell metacharacters in the nagios_path parameter to lilac/ex demonstrated by %26%26+curl to insert an "&& curl" substring for the shell.

CVE Number	Description
CVE-2021-21549	Dell EMC XtremIO Versions prior to 6.3.3-8, contain a Cross-Site Request Forgery Vulnerability in XMS. A non-privileged attacker could potentially exploit this vulnerab privileged victim application user being tricked into sending state-changing requests to the vulnerable application, causing unintended server operations.
CVE-2021-24307	The All in One SEO – Best WordPress SEO Plugin – Easily Improve Your SEO Rankings before 4.1.0.2 enables authenticated users with "aioseo_tools_settings" privil admin) to execute arbitrary code on the underlying host. Users can restore plugin's configuration by uploading a backup .ini file in the section "Tool > Import/Export". Ho attempts to unserialize values of the .ini file. Moreover, the plugin embeds Monolog library which can be used to craft a gadget chain and thus trigger system command
CVE-2021-30081	An issue was discovered in emlog 6.0.0stable. There is a SQL Injection vulnerability that can execute any SQL statement and query server sensitive data via admin/na action=add_page.
CVE-2021-29256	. The Arm Mali GPU kernel driver allows an unprivileged user to achieve access to freed memory, leading to information disclosure or root privilege escalation. This affe through r29p0 before r30p0, Valhall r19p0 through r29p0 before r30p0, and Midgard r28p0 through r30p0.
CVE-2021-28798	A relative path traversal vulnerability has been reported to affect QNAP NAS running QTS and QuTS hero. If exploited, this vulnerability allows attackers to modify files integrity. QNAP have already fixed this vulnerability in the following versions: QTS 4.5.2.1630 Build 20210406 and later QTS 4.3.6.1663 Build 20210504 and later QTS 20210416 and later QuTS hero h4.5.2.1638 Build 20210414 and later QNAP NAS running QTS 4.5.3 are not affected.
CVE-2020-28906	Incorrect File Permissions in Nagios XI 5.7.5 and earlier and Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation to root. Low-privileged users are able to mo included (aka sourced) by scripts executed by root.
CVE-2020-28909	Incorrect File Permissions in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation to root via modification of scripts. Low-privileges users are able to modify fil executed by sudo.
CVE-2020-26559	Bluetooth Mesh Provisioning in the Bluetooth Mesh profile 1.0 and 1.0.1 may permit a nearby device (participating in the provisioning protocol) to identify the AuthValue Provisioner's public key, and the confirmation number and nonce provided by the provisioning device. This could permit a device without the AuthValue to complete pro brute-forcing the AuthValue.
CVE-2021-21657	Jenkins Filesystem Trigger Plugin 0.40 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.
CVE-2017-17677	BMC Remedy 9.1SP3 is affected by authenticated code execution. Authenticated users that have the right to create reports can use BIRT templates to run code.
CVE-2021-28111	Draeger X-Dock Firmware before 03.00.13 has Hard-Coded Credentials, leading to remote code execution by an authenticated attacker.
CVE-2020-4990	IBM Security Guardium 11.2 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add information in the back-end database. IBM X-Force ID: 192710.
CVE-2021-33477	rxvt-unicode 9.22, rxvt 2.7.10, mrxvt 0.5.4, and Eterm 0.9.7 allow (potentially remote) code execution because of improper handling of certain escape sequences (ESC terminated by a newline.
CVE-2021-3517	There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is able to supply a crafted file to be processed by an applica affected functionality of libxml2 could trigger an out-of-bounds read. The most likely impact of this flaw is to application availability, with some potential impact to confide an attacker is able to use memory information to further exploit the application.
CVE-2020-10064	Improper Input Frame Validation in ieee802154 Processing. Zephyr versions >= v1.14.2, >= v2.2.0 contain Stack-based Buffer Overflow (CWE-121), Heap-based Buffe 122). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-3gvq-h42f-v3c7
CVE-2021-20096	Cross-site request forgery in OpenOversight 0.6.4 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link
CVE-2021-21659	Jenkins URLTrigger Plugin 0.48 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.
CVE-2020-21057	Directory Traversal vulnerability in FusionPBX 4.5.7, which allows a remote malicious user to delete folders on the system via the folder variable to app/edit/folderdelete
CVE-2021-29503	HedgeDoc is a platform to write and share markdown. HedgeDoc before version 1.8.2 is vulnerable to a cross-site scripting attack using the YAML-metadata of a note. access to a note can embed HTML tags in the Open Graph metadata section of the note, resulting in the frontend rendering the script tag as part of the `<head>` sectio instance prevents guests from editing notes, this vulnerability allows unauthenticated attackers to inject JavaScript into notes that allow guest edits. If your instance pre editing notes, this vulnerability allows authenticated attackers to inject JavaScript into any note pages they have write-access to. This vulnerability is patched in version workaround, one can disable guest edits until the next update.

CVE Number	Description
CVE-2021-33516	An issue was discovered in GUPnP before 1.0.7 and 1.1.x and 1.2.x before 1.2.5. It allows DNS rebinding. A remote web server can exploit this vulnerability to trick a v triggering actions against local UPnP services implemented using this library. Depending on the affected service, this could be used for data exfiltration, data tempering
CVE-2020-26560	Bluetooth Mesh Provisioning in the Bluetooth Mesh profile 1.0 and 1.0.1 may permit a nearby device, reflecting the authentication evidence from a Provisioner, to comp without possessing the AuthValue, and potentially acquire a NetKey and AppKey.
CVE-2020-9452	An issue was discovered in Acronis True Image 2020 24.5.22510. anti_ransomware_service.exe includes functionality to quarantine files by copying a suspected ranso directory to another using SYSTEM privileges. Because unprivileged users have write permissions in the quarantine folder, it is possible to control this privileged write v means that an unprivileged user can write/overwrite arbitrary files in arbitrary folders. Escalating privileges to SYSTEM is trivial with arbitrary writes. While the quarantir enabled by default, it can be forced to copy the file to the quarantine by communicating with anti_ransomware_service.exe through its REST API.
CVE-2021-31473	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vul target must visit a malicious page or open a malicious file. The specific flaw exists within the browseForDoc function. The issue results from the lack of proper validatior data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current proc 13523.
CVE-2021-20389	IBM Security Guardium 11.2 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 195770.
CVE-2021-3438	A potential buffer overflow in the software drivers for certain HP LaserJet products and Samsung product printers could lead to an escalation of privilege.
CVE-2020-9450	An issue was discovered in Acronis True Image 2020 24.5.22510. anti_ransomware_service.exe exposes a REST API that can be used by everyone, even unprivilege used to communicate from the GUI to anti_ransomware_service.exe. This can be exploited to add an arbitrary malicious executable to the whitelist, or even exclude an being monitored by anti_ransomware_service.exe.
CVE-2021-20713	Privilege escalation vulnerability in QND Advance/Premium/Standard Ver.11.0.4i and earlier allows an attacker who can log in to the PC where the product's Windows gain administrative privileges via unspecified vectors. As a result, sensitive information may be altered/obtained or unintended operations may be performed.
CVE-2021-20722	Untrusted search path vulnerability in the installers of ScanSnap Manager prior to versions V7.0L20 and the Software Download Installer prior to WinSSInst2JP.exe an WinSSInst2iX1500JP.exe allows an attacker to gain privileges and execute arbitrary code with the privilege of the user invoking the installer via a Trojan horse DLL in a directory.
CVE-2021-20726	Untrusted search path vulnerability in The Installer of Overwolf 2.168.0.n and earlier allows an attacker to gain privileges and execute arbitrary code with the privilege o the installer via a Trojan horse DLL in an unspecified directory.
CVE-2021-23386	This affects the package dns-packet before 5.2.2. It creates buffers with allocUnsafe and does not always fill them before forming network packets. This can expose int memory over unencrypted network when querying crafted invalid domain names.
CVE-2021-33500	PuTTY before 0.75 on Windows allows remote servers to cause a denial of service (Windows GUI hang) by telling the PuTTY window to change its title repeatedly at h results in many SetWindowTextA or SetWindowTextW calls. NOTE: the same attack methodology may affect some OS-level GUIs on Linux or other platforms for simil
CVE-2020-27209	The ECDSA operation of the micro-ecc library 1.0 is vulnerable to simple power analysis attacks which allows an adversary to extract the private ECC key.
CVE-2021-29258	An issue was discovered in Envoy 1.14.0. There is a remotely exploitable crash for HTTP2 Metadata, because an empty METADATA map triggers a Reachable Assert
CVE-2020-21041	Buffer Overflow vulnerability exists in FFmpeg 4.1 via apng_do_inverse_blend in libavcodec/pngenc.c, which could let a remote malicious user cause a Denial of Servic
CVE-2021-28902	In function read_yin_container() in libyang <= v1.0.225, it doesn't check whether the value of retval->ext[r] is NULL. In some cases, it can be NULL, which leads to the >ext[r]->flags that results in a crash.
CVE-2021-28903	A stack overflow in libyang <= v1.0.225 can cause a denial of service through function lyxml_parse_mem(). lyxml_parse_elem() function will be called recursively, whic space and lead to crash.
CVE-2021-28904	In function ext_get_plugin() in libyang <= v1.0.225, it doesn't check whether the value of revision is NULL. If revision is NULL, the operation of strcmp(revision, ext_plug lead to a crash.

CVE Number	Description
CVE-2021-32624	Keystone 5 is an open source CMS platform to build Node.js applications. This security advisory relates to a newly discovered capability in our query infrastructure to di expose the values of private fields, bypassing the configured access control. This is an access control related oracle attack in that the attack method guides an attacker to reveal information they do not have access to. The complexity of completing the attack is limited by some length-dependent behaviors and the fidelity of the exposed some circumstances, field values or field value meta data can be determined, despite the field or list having `read` access control configured. If you use private fields or impacted. No patches exist at this time. There are no workarounds at this time
CVE-2021-28905	In function lys_node_free() in libyang <= v1.0.225, it asserts that the value of node->module can't be NULL. But in some cases, node->module can be null, which trigge assertion (CWE-617).
CVE-2021-28906	In function read_yin_leaf() in libyang <= v1.0.225, it doesn't check whether the value of retval->ext[r] is NULL. In some cases, it can be NULL, which leads to the operat >flags that results in a crash.
CVE-2020-18220	Weak Encoding for Password in DoraCMS v2.1.1 and earlier allows attackers to obtain sensitive information as it does not use a random salt or IV for its AES-CBC enc password encrypted for users to be susceptible to dictionary attacks.
CVE-2021-33502	The normalize-url package before 4.5.1, 5.x before 5.3.1, and 6.x before 6.0.1 for Node.js has a ReDoS (regular expression denial of service) issue because it has exp for data: URLs.
CVE-2021-20419	IBM Security Guardium 11.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID:
CVE-2020-20178	Ethereum 0xe933c0cd9784414d5f278c114904f5a84b396919#code.sol latest version is affected by a denial of service vulnerability in the affected payout function. Onc array is too long, it will result in an exception. Attackers can make attacks by creating a series of account addresses.
CVE-2020-23768	An information disclosure vulnerability was discovered in alipay_function.php in the log file of Alibaba payment interface on PHPPYUN prior to version 5.0.1. If exploited allow attackers to obtain users' personally identifiable information including e-mail address and telephone numbers.
CVE-2021-33563	Koel before 5.1.4 lacks login throttling, lacks a password strength policy, and shows whether a failed login attempt had a valid username. This might make brute-force a
CVE-2021-32032	In Trusted Firmware-M through 1.3.0, cleaning up the memory allocated for a multi-part cryptographic operation (in the event of a failure) can prevent the abort() operat cryptographic library from freeing internal resources, causing a memory leak.
CVE-2020-26557	Mesh Provisioning in the Bluetooth Mesh profile 1.0 and 1.0.1 may permit a nearby device (without possession of the AuthValue used in the provisioning protocol) to de AuthValue via a brute-force attack (unless the AuthValue is sufficiently random and changed each time).
CVE-2021-21732	A mobile phone of ZTE is impacted by improper access control vulnerability. Due to improper permission settings, third-party applications can read some files in the pro authorization. Attackers could exploit this vulnerability to obtain sensitive information. This affects Axon 11 5G ZTE/CN_P725A12/P725A12:10/QKQ1.200816.002/20201116.175317:user/release-keys.
CVE-2021-30186	CODESYS V2 runtime system SP before 2.4.7.55 has a Heap-based Buffer Overflow.
CVE-2021-30191	CODESYS V2 Web-Server before 1.1.9.20 has a a Buffer Copy without Checking the Size of the Input.
CVE-2021-30195	CODESYS V2 runtime system before 2.4.7.55 has Improper Input Validation.
CVE-2020-36332	A flaw was found in libwebp in versions before 1.0.1. When reading a file libwebp allocates an excessive amount of memory. The highest threat from this vulnerability is availability.
CVE-2021-28683	An issue was discovered in Envoy through 1.71.1. There is a remotely exploitable NULL pointer dereference and crash in TLS when an unknown TLS alert code is rece
CVE-2021-27823	An information disclosure vulnerability was discovered in /index.class.php (via port 8181) on NetWave System 1.0 which allows unauthenticated attackers to exfiltrate s from the system.
CVE-2021-33511	Plone though 5.2.4 allows SSRF via the lxml parser. This affects Diazo themes, Dexterity TTW schemas, and modeleditors in plone.app.theming, plone.app.dexterity, a plone.supermodel.

CVE Number	Description
CVE-2021-20589	Buffer access with incorrect length value vulnerability in GOT2000 series GT27 model communication driver versions 01.19.000 through 01.38.000, GT25 model comm versions 01.19.000 through 01.38.000, GT23 model communication driver versions 01.19.000 through 01.38.000 and GT21 model communication driver versions 01.2 01.39.000, GOT SIMPLE series GS21 model communication driver versions 01.21.000 through 01.39.000, GT SoftGOT2000 versions 1.170C through 1.250L and Ten 40GU-L Screen package data for MODBUS/TCP V1.00 allows a remote unauthenticated attacker to stop the communication function of the products via specially craft
CVE-2020-26556	Mesh Provisioning in the Bluetooth Mesh profile 1.0 and 1.0.1 may permit a nearby device, able to conduct a successful brute-force attack on an insufficiently random A provisioning procedure times out, to complete authentication by leveraging Malleable Commitment.
CVE-2021-28682	An issue was discovered in Envoy through 1.71.1. There is a remotely exploitable integer overflow in which a very large grpc-timeout value leads to unexpected timeou
CVE-2021-3480	A flaw was found in slapi-nis in versions before 0.56.7. A NULL pointer dereference during the parsing of the Binding DN could allow an unauthenticated attacker to cra directory server. The highest threat from this vulnerability is to system availability.
CVE-2020-20450	FFmpeg 4.2 is affected by null pointer dereference passed as argument to libavformat/aviobuf.c, which could cause a Denial of Service.
CVE-2021-27461	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver applications allow access to stored data by using specially crafted URLs.
CVE-2021-27457	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for sto data, which may allow an attacker to more easily obtain credentials used for access.
CVE-2021-20718	mod_auth_openidc 2.4.0 to 2.4.7 allows a remote attacker to cause a denial-of-service (DoS) condition via unspecified vectors.
CVE-2021-29625	Adminer is open-source database management software. A cross-site scripting vulnerability in Adminer versions 4.6.1 to 4.8.0 affects users of MySQL, MariaDB, PgSC in most cases prevented by strict CSP in all modern browsers. The only exception is when Adminer is using a `pdo_` extension to communicate with the database (it is extensions are not enabled). In browsers without CSP, Adminer versions 4.6.1 to 4.8.0 are affected. The vulnerability is patched in version 4.8.1. As workarounds, one supporting strict CSP or enable the native PHP extensions (e.g. `mysqli`) or disable displaying PHP errors (`display_errors`).
CVE-2020-20451	Denial of Service issue in FFmpeg 4.2 due to resource management errors via fftools/cmdutils.c.
CVE-2020-25672	A memory leak vulnerability was found in Linux kernel in llcp_sock_connect
CVE-2021-25644	An issue was discovered in Couchbase Server 5.x and 6.x through 6.6.1 and 7.0.0 Beta. Incorrect commands to the REST API can result in leaked authentication infor cleartext in the debug.log and info.log files, and is also shown in the UI visible to administrators.
CVE-2021-29688	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. T be used in further attacks against the system. IBM X-Force ID: 200102.
CVE-2021-29691	IBM Security Identity Manager 7.0.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbo external components, or encryption of internal data. IBM X-Force ID: 200252.
CVE-2020-24396	homee Brain Cube v2 (2.28.2 and 2.28.4) devices have sensitive SSH keys within downloadable and unencrypted firmware images. This allows remote attackers to us as a SOCKS proxy.
CVE-2021-3445	A flaw was found in libdnf's signature verification functionality in versions before 0.60.1. This flaw allows an attacker to achieve code execution if they can alter the hea RPM package and then trick a user or system into installing it. The highest risk of this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2021-27434	Products with Unified Automation .NET based OPC UA Client/Server SDK Bundle: Versions V3.0.7 and prior (.NET 4.5, 4.0, and 3.5 Framework versions only) are vulr uncontrolled recursion, which may allow an attacker to trigger a stack overflow.
CVE-2021-23937	A DNS proxy and possible amplification attack vulnerability in WebClientInfo of Apache Wicket allows an attacker to trigger arbitrary DNS lookups from the server when header is not properly sanitized. This DNS lookup can be engineered to overload an internal DNS server or to slow down request processing of the Apache Wicket app possible denial of service on either the internal infrastructure or the web application itself. This issue affects Apache Wicket Apache Wicket 9.x version 9.2.0 and prior v Wicket 8.x version 8.11.0 and prior versions; Apache Wicket 7.x version 7.17.0 and prior versions and Apache Wicket 6.x version 6.2.0 and later versions.

CVE Number	Description
CVE-2020-35580	A local file inclusion vulnerability in the FileServlet in all SearchBlox before 9.2.2 allows remote, unauthenticated users to read arbitrary files from the operating system /searchblox/servlet/FileServlet?col=url= request. Additionally, this may be used to read the contents of the SearchBlox configuration file (e.g., searchblox/WEB-INF/con contains both the Super Admin's API key and the base64 encoded SHA1 password hashes of other SearchBlox users.
CVE-2021-27432	OPC Foundation UA .NET Standard versions prior to 1.4.365.48 and OPC UA .NET Legacy are vulnerable to an uncontrolled recursion, which may allow an attacker to overflow.
CVE-2021-20209	A memory leak vulnerability was found in Privoxy before 3.0.29 in the show-status CGI handler when no action files are configured.
CVE-2016-20011	libgrss through 0.7.0 fails to perform TLS certificate verification when downloading feeds, allowing remote attackers to manipulate the contents of feeds without detectio because of the default behavior of SoupSessionSync.
CVE-2020-4850	IBM Spectrum Scale 1.1.1.0 through 1.1.8.4 Transparent Cloud Tiering could allow a remote attacker to obtain sensitive information, caused by the leftover files after c Force ID: 190298.
CVE-2021-27811	A code injection vulnerability has been discovered in the Upgrade function of QibosoftX1 v1.0. An attacker is able execute arbitrary PHP code via exploitation of client_ and Upgrade.php.
CVE-2020-23765	A file upload vulnerability was discovered in the file path /bl-plugins/backup/plugin.php on Bludit version 3.12.0. If an attacker is able to gain Administrator rights they wi unsafe plugins to upload a backup file and control the server.
CVE-2021-32634	Emissary is a distributed, peer-to-peer, data-driven workflow framework. Emissary 6.4.0 is vulnerable to Unsafe Deserialization of post-authenticated requests to the [`WorkSpaceClientEnqueue.action`] (https://github.com/NationalSecurityAgency/emissary/blob/30c54ef16c6eb6ed09604a929939fb9f66868382/src/main/java/emissary/server/mvc/internal/WorkSpaceClier REST endpoint. This issue may lead to post-auth Remote Code Execution. This issue has been patched in version 6.5.0. As a workaround, one can disable network ac from untrusted sources.
CVE-2021-20385	IBM Security Guardium 11.2 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an atta vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 195766.
CVE-2021-20557	IBM Security Guardium 11.2 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-F
CVE-2021-32629	Cranelift is an open-source code generator maintained by Bytecode Alliance. It translates a target-independent intermediate representation into executable machine co 0.73 of the Cranelift x64 backend that can create a scenario that could result in a potential sandbox escape in a Wasm program. This bug was introduced in the new ba and first included in a release on 2020-09-30, but the new backend was not the default prior to 0.73. The recently-released version 0.73 with default settings, and prior explicit build flag to select the new backend, are vulnerable. The bug in question performs a sign-extend instead of a zero-extend on a value loaded from the stack, und circumstances. If those circumstances occur, the bug could allow access to memory addresses upto 2GiB before the start of the Wasm program heap. If the heap bour then it would be possible to read memory from a computable range dependent on the size of the heaps bound. The impact of this bug is highly dependent on heap impl specifically: * if the heap has bounds checks, and * does not rely exclusively on guard pages, and * the heap bound is 2GiB or smaller * then this bug cannot be used to another Wasm program heap. The impact of the vulnerability is mitigated if there is no memory mapped in the range accessible using this bug, for example, if there is a before the Wasm program heap. The bug in question performs a sign-extend instead of a zero-extend on a value loaded from the stack, when the register allocator relo value narrower than 64 bits. This interacts poorly with another optimization: the instruction selector elides a 32-to-64-bit zero-extend operator when we know that an ins 32-bit value actually zeros the upper 32 bits of its destination register. Hence, we rely on these zeroed bits, but the type of the value is still i32, and the spill/reload reco the sign extension of the i32's MSB. The issue would thus occur when: * An i32 value in a Wasm program is greater than or equal to 0x8000_0000; * The value is spille the register allocator due to high register pressure in the program between the value's definition and its use; * The value is produced by an instruction that we know to b zeroes the upper 32 bits of its destination: add, sub, mul, and, or; * The value is then zero-extended to 64 bits in the Wasm program; * The resulting 64-bit value is used circumstances there is a potential sandbox escape when the i32 value is a pointer. The usual code emitted for heap accesses zero-extends the Wasm heap address, a base, and accesses the resulting address. If the zero-extend becomes a sign-extend, the program could reach backward and access memory up to 2GiB before the sta addition to assessing the nature of the code generation bug in Cranelift, we have also determined that under specific circumstances, both Lucet and Wasmtime using th may be exploitable. See referenced GitHub Advisory for more details.
CVE-2021-31440	This vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel 5.11.15. An attacker must first obtain the ability to execute low-pri target system in order to exploit this vulnerability. The specific flaw exists within the handling of eBPF programs. The issue results from the lack of proper validation of u programs prior to executing them. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel. Was ZDI-CAI
CVE-2020-13600	Malformed SPI in response for eswifi can corrupt kernel memory. Zephyr versions >= 1.14.2, >= 2.3.0 contain Heap-based Buffer Overflow (CWE-122). For more inform https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-hx4p-j86p-2mhr
CVE-2020-27212	STMicroelectronics STM32L4 devices through 2020-10-19 have incorrect access control. The flash read-out protection (RDP) can be degraded from RDP level 2 (no a interface) to level 1 (limited access via debug interface) by injecting a fault during the boot phase.
CVE-2020-13603	Integer Overflow in memory allocating functions. Zephyr versions >= 1.14.2, >= 2.4.0 contain Integer Overflow or Wraparound (CWE-190). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-94vp-8gc2-rm45

CVE Number	Description
CVE-2020-24395	The USB firmware update script of homee Brain Cube v2 (2.28.2 and 2.28.4) devices allows an attacker with physical access to install compromised firmware. This occ insufficient validation of the firmware image file and can lead to code execution on the device.
CVE-2021-20719	RFNTPS firmware versions System_01000004 and earlier, and Web_01000004 and earlier allow an attacker on the same network segment to execute arbitrary OS co privilege via unspecified vectors.
CVE-2021-32633	Zope is an open-source web application server. In Zope versions prior to 4.6 and 5.2, users can access untrusted modules indirectly through Python modules that are a use. By default, only users with the Manager role can add or edit Zope Page Templates through the web, but sites that allow untrusted users to add/edit Zope Page Ter web are at risk from this vulnerability. The problem has been fixed in Zope 5.2 and 4.6. As a workaround, a site administrator can restrict adding/editing Zope Page Ter web using the standard Zope user/role permission mechanisms. Untrusted users should not be assigned the Zope Manager role and adding/editing Zope Page Templa should be restricted to trusted users only.
CVE-2020-27208	The flash read-out protection (RDP) level is not enforced during the device initialization phase of the SoloKeys Solo 4.0.0 & Somu and the Nitrokey FIDO2 token. This a downgrade the RDP level and access secrets such as private ECC keys from SRAM via the debug interface.
CVE-2021-29708	IBM Spectrum Scale 5.1.0.1 could allow a local with access to the GUI pod container to obtain sensitive cryptographic keys that could allow them to elevate their privile 200883.
CVE-2021-29202	A local buffer overflow vulnerability was discovered in HPE Integrated Lights-Out 4 (iLO 4); HPE SimpliVity 380 Gen9; HPE Integrated Lights-Out 5 (iLO 5) for HPE Ge SimpliVity 380 Gen10; HPE SimpliVity 2600; HPE SimpliVity 380 Gen10 G; HPE SimpliVity 325; HPE SimpliVity 380 Gen10 H version(s): Prior to version 2.78.
CVE-2020-25408	A Cross-Site Request Forgery (CSRF) vulnerability exists in ProjectWorlds College Management System Php 1.0 that allows a remote attacker to modify, delete, or ma student, faculty, teacher, subject, scores, location, and article data.
CVE-2021-29624	fastify-csrf is an open-source plugin helps developers protect their Fastify server against CSRF attacks. Versions of fastify-csrf prior to 3.1.0 have a "double submit" me cookies with an application deployed across multiple subdomains, e.g. "heroku"-style platform as a service. Version 3.1.0 of the fastify-csrf fixes it. the vulnerability. The would need to supply a `userInfo` when generating the CSRF token to fully implement the protection on their end. This is needed only for applications hosted on differe
CVE-2021-29622	Prometheus is an open-source monitoring system and time series database. In 2.23.0, Prometheus changed its default UI to the New ui. To ensure a seamless transitio by /new redirect to /. Due to a bug in the code, it is possible for an attacker to craft an URL that can redirect to any other URL, in the /new endpoint. If a user visits a pro a specially crafted address, they can be redirected to an arbitrary URL. The issue was patched in the 2.26.1 and 2.27.1 releases. In 2.28.0, the /new endpoint will be re The workaround is to disable access to /new via a reverse proxy in front of Prometheus.
CVE-2020-20453	FFmpeg 4.2 is affected by a Divide By Zero issue via libavcodec/aaccoder, which allows a remote malicious user to cause a Denial of Service
CVE-2021-21987	VMware Workstation (16.x prior to 16.1.2) and Horizon Client for Windows (5.x prior to 5.5.2) contain out-of-bounds read vulnerability in the Cortado ThinPrint compone malicious actor with access to a virtual machine or remote desktop may be able to exploit these issues leading to information disclosure from the TPView process runni where Workstation or Horizon Client for Windows is installed.
CVE-2021-21988	VMware Workstation (16.x prior to 16.1.2) and Horizon Client for Windows (5.x prior to 5.5.2) contain out-of-bounds read vulnerability in the Cortado ThinPrint compone Parser). A malicious actor with access to a virtual machine or remote desktop may be able to exploit these issues leading to information disclosure from the TPView pro system where Workstation or Horizon Client for Windows is installed.
CVE-2021-21989	VMware Workstation (16.x prior to 16.1.2) and Horizon Client for Windows (5.x prior to 5.5.2) contain out-of-bounds read vulnerability in the Cortado ThinPrint compone malicious actor with access to a virtual machine or remote desktop may be able to exploit these issues leading to information disclosure from the TPView process runni where Workstation or Horizon Client for Windows is installed.
CVE-2021-3559	A flaw was found in libvirt in the virConnectListAllNodeDevices API in versions before 7.0.0. It only affects hosts with a PCI device and driver that supports mediated de driver). This flaw could be used by an unprivileged client with a read-only connection to crash the libvirt daemon by executing the 'nodedev-list' virsh command. The hig vulnerability is to system availability.
CVE-2020-25411	Projectworlds Online Examination System 1.0 is vulnerable to CSRF, which allows a remote attacker to delete the existing user.
CVE-2021-1559	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, remote attacker to perform a command injection attack on an affected device. Th due to insufficient input sanitization when executing affected commands. A high-privileged attacker could exploit these vulnerabilities on a Cisco DNA Spaces Connecto input during command execution. A successful exploit could allow the attacker to execute arbitrary commands as root within the Connector docker container.
CVE-2021-31158	In the Query Engine in Couchbase Server 6.5.x and 6.6.x through 6.6.1, Common Table Expression queries were not correctly checking the user's permissions, allowin resources beyond what those users were explicitly allowed to access.
CVE-2021-29683	IBM Security Identity Manager 7.0.2 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 199998.
CVE-2021-29695	IBM Host firmware for LC-class Systems could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request th to delete arbitrary files on the system. IBM X-Force ID: 200558.

CVE Number	Description
CVE-2020-28911	Incorrect Access Control in Nagios Fusion 4.1.8 and earlier allows low-privileged authenticated users to extract passwords used to manage fused servers via the test_s ajaxhelper.php.
CVE-2021-22339	There is a denial of service vulnerability in some versions of ManageOne. In specific scenarios, due to the insufficient verification of the parameter, an attacker may cra parameter. Successful exploit may cause some services abnormal.
CVE-2020-21055	A Directory Traversal vulnerability exists in FusionPBX 4.5.7 allows malicoius users to rename any file of the system.via the (1) folder, (2) filename, and (3) newfilenam app\edit\filerename.php.
CVE-2020-20266	Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/dot1x process. An authenticated remote attacker can cause a (NULL pointer dereference).
CVE-2020-20264	Mikrotik RouterOs before 6.47 (stable tree) in the /ram/pckg/advanced-tools/nova/bin/netwatch process. An authenticated remote attacker can cause a Denial of Servic zero error.
CVE-2021-1560	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, remote attacker to perform a command injection attack on an affected device. Th due to insufficient input sanitization when executing affected commands. A high-privileged attacker could exploit these vulnerabilities on a Cisco DNA Spaces Connecto input during command execution. A successful exploit could allow the attacker to execute arbitrary commands as root within the Connector docker container.
CVE-2020-20446	FFmpeg 4.2 is affected by a Divide By Zero issue via libavcodec/aacpsy.c, which allows a remote malicious user to cause a Denial of Service.
CVE-2020-23766	An arbitrary file deletion vulnerability was discovered on htmly v2.7.5 which allows remote attackers to use any absolute path to delete any file in the server should they privileges.
CVE-2021-29659	ownCloud 10.7 has an incorrect access control vulnerability, leading to remote information disclosure. Due to a bug in the related API endpoint, the attacker can enume single request by entering three whitespaces. Secondary, the retrieval of all users on a large instance could cause higher than average load on the instance.
CVE-2020-20445	FFmpeg 4.2 is affected by a Divide By Zero issue via libavcodec/lpc.h, which allows a remote malicious user to cause a Denial of Service.
CVE-2020-20448	FFmpeg 4.1.3 is affected by a Divide By Zero issue via libavcodec/ratecontrol.c, which allows a remote malicious user to cause a Denial of Service.
CVE-2021-3485	An Improper Input Validation vulnerability in the Product Update feature of Bitdefender Endpoint Security Tools for Linux allows a man-in-the-middle attacker to abuse t function of the Product Update to achieve remote code execution. This issue affects: Bitdefender Endpoint Security Tools for Linux versions prior to 6.2.21.155.
CVE-2020-13598	FS: Buffer Overflow when enabling Long File Names in FAT_FS and calling fs_stat. Zephyr versions >= v1.14.2, >= v2.3.0 contain Stack-based Buffer Overflow (CWE- information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-7fhv-rgxr-x56h
CVE-2021-27465	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not validate webpage input, which c attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data.
CVE-2020-21053	Cross Site Scriptiong (XSS) vulnerability exists in FusionPBX 4.5.7 allows remote malicious users to inject arbitrary web script or HTML via an unsanitized "query_string app\devices\device_imports.php.
CVE-2021-27821	The Web Interface for OpenWRT LuCI version 19.07 and lower has been discovered to have a cross-site scripting vulnerability which can lead to attackers carrying out execution.
CVE-2020-26006	Project Worlds Online Examination System 1.0 is affected by Cross Site Scripting (XSS) via account.php.
CVE-2020-28903	Improper input validation in Nagios Fusion 4.1.8 and earlier allows a remote attacker with control over a fused server to inject arbitrary HTML, aka XSS.

CVE Number	Description
CVE-2021-20386	IBM Security Guardium 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the inten potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195767.
CVE-2020-36365	Smartstore (aka SmartStoreNET) before 4.1.0 allows CommonController.ClearCache, ClearDatabaseCache, RestartApplication, and ScheduleTaskController.Edit oper
CVE-2021-25938	In ArangoDB, versions v2.2.6.2 through v3.7.10 are vulnerable to Cross-Site Scripting (XSS), since there is no validation of the .zip file name and filtering of potential al which zip files can be named to. There is no X-Frame-Options Header set, which makes it more susceptible for leveraging self XSS by attackers.
CVE-2021-31930	Persistent cross-site scripting (XSS) in the web interface of Concerto through 2.3.6 allows an unauthenticated remote attacker to introduce arbitrary JavaScript by inject into the First Name or Last Name parameter upon registration. When a privileged user attempts to delete the account, the XSS payload will be executed.
CVE-2020-21054	Cross Site Scripting (XSS) vulnerability in FusionPBX 4.5.7 allows remote malicious users to inject arbitrary web script or HTML via an unsanitized "f" variable in app\va
CVE-2017-17678	BMC Remedy Mid Tier 9.1SP3 is affected by cross-site scripting (XSS). A DOM-based cross-site scripting vulnerability was discovered in a legacy utility.
CVE-2021-27956	Zoho ManageEngine ADSelfService Plus before 6104 allows stored XSS on the /webclient/index.html#/directory-search user search page via the e-mail address field.
CVE-2021-33507	Zope Products.CMFCore before 2.5.1 and Products.PluggableAuthService before 2.6.2, as used in Plone through 5.2.4 and other products, allow Reflected XSS.
CVE-2021-27467	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product's web interface allows an attacker to route another page provided by the attacker to gain unauthorized access to sensitive information.
CVE-2021-24297	The Goto WordPress theme before 2.1 did not properly sanitize the formvalue JSON POST parameter in its tl_filter AJAX action, leading to an unauthenticated Reflecte Scripting (XSS) vulnerability.
CVE-2021-24294	The dsgvoaio_write_log AJAX action of the DSGVO All in one for WP WordPress plugin before 4.0 did not sanitise or escape some POST parameter submitted before Log page in the administrator dashboard (wp-admin/admin.php?page=dsgvoaiofree-show-log). This could allow unauthenticated attackers to gain unauthorised access payload to create a rogue administrator account, which will be trigged when an administrator will view the logs.
CVE-2021-33496	Dutchcoders transfer.sh before 1.2.4 allows XSS via an inline view.
CVE-2021-29414	STMicroelectronics STM32L4 devices through 2021-03-29 have incorrect physical access control.
CVE-2021-30082	An issue was discovered in Gris CMS v0.1. There is a Persistent XSS vulnerability which allows remote attackers to inject arbitrary web script or HTML via admin/dashl
CVE-2020-21345	Cross Site Scripting (XSS) vulnerability in Halo 1.1.3 via post publish components in the manage panel, which lets a remote malicious user execute arbitrary code.
CVE-2021-20723	Reflected cross-site scripting vulnerability in [MailForm01] free edition (versions which the last updated date listed at the top of descriptions in the program file is from 2 2018 July 27) allows a remote attacker to inject an arbitrary script via unspecified vectors.
CVE-2021-24305	The Target First WordPress Plugin v2.0, also previously known as Watcheezy, suffers from a critical unauthenticated stored XSS vulnerability. An attacker could chang value through a POST on any URL with the 'weeWzKey' parameter that will be save as the 'weeID option and is not sanitized.
CVE-2021-30083	An issue was discovered in Mediat 1.4.1. There is a Reflected XSS vulnerability which allows remote attackers to inject arbitrary web script or HTML without authentica parameter in login.php.
CVE-2021-20724	Reflected cross-site scripting vulnerability in the admin page of [Telop01] free edition ver1.0.1 and earlier allows a remote attacker to inject an arbitrary script via unspe

CVE Number	Description
CVE-2021-20725	Reflected cross-site scripting vulnerability in the admin page of [Calendar01] free edition ver1.0.1 and earlier allows a remote attacker to inject an arbitrary script via uns
CVE-2021-24300	The slider import search feature of the PickPlugins Product Slider for WooCommerce WordPress plugin before 1.13.22 did not properly sanitised the keyword GET para reflected Cross-Site Scripting issue
CVE-2021-24298	The method and share GET parameters of the Giveaway pages were not sanitised, validated or escaped before being output back in the pages, thus leading to reflecte
CVE-2021-1557	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the under system as root. These vulnerabilities are due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities by insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin and execute arbitrary co underlying operating system as root.
CVE-2021-1558	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the under system as root. These vulnerabilities are due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities by insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin and execute arbitrary co underlying operating system as root.
CVE-2021-3320	Type Confusion in 802154 ACK Frames Handling. Zephyr versions >= v2.4.0 contain NULL Pointer Dereference (CWE-476). For more information, see https://github.co rtos/zephyr/security/advisories/GHSA-27r3-rxch-2hm7
CVE-2020-15522	Bouncy Castle BC Java before 1.66, BC C# .NET before 1.8.7, BC-FJA before 1.0.1.2, 1.0.2.1, and BC-FNA before 1.0.1.1 have a timing issue within the EC math libra information about the private key when an attacker is able to observe timing information for the generation of multiple deterministic ECDSA signatures.
CVE-2021-29692	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Securi exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 200253.
CVE-2008-3280	It was found that various OpenID Providers (OPs) had TLS Server Certificates that used weak keys, as a result of the Debian Predictable Random Number Generator (combination with the DNS Cache Poisoning issue (CVE-2008-1447) and the fact that almost all SSL/TLS implementations do not consult CRLs (currently an untracked that it is impossible to rely on these OPs.
CVE-2021-27924	An issue was discovered in Couchbase Server 6.x through 6.6.1. The Couchbase Server UI is insecurely logging session cookies in the logs. This allows for the impers the log files are obtained by an attacker before a session cookie expires.
CVE-2020-10072	Improper Handling of Insufficient Permissions or Privileges in zephyr. Zephyr versions >= v1.14.2, >= v2.2.0 contain Improper Handling of Insufficient Permissions or Pr For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-vf79-hqwm-w4xc
CVE-2021-3426	There's a flaw in Python 3's pydoc. A local or adjacent attacker who discovers or is able to convince another local or adjacent user to start a pydoc server could access to disclose sensitive information belonging to the other user that they would not normally be able to access. The highest risk of this flaw is to data confidentiality. This fla versions before 3.8.9, Python versions before 3.9.3 and Python versions before 3.10.0a7.
CVE-2020-27211	Nordic Semiconductor nRF52840 devices through 2020-10-19 have improper protection against physical side channels. The flash read-out protection (APPROTECT) c injecting a fault during the boot phase.
CVE-2021-27562	In Arm Trusted Firmware M through 1.2, the NS world may trigger a system halt, an overwrite of secure data, or the printing out of secure data when calling secure func NSPE handler mode.
CVE-2021-3421	A flaw was found in the RPM package in the read functionality. This flaw allows an attacker who can convince a victim to install a seemingly verifiable package or comp repository, to cause RPM database corruption. The highest threat from this vulnerability is to data integrity. This flaw affects RPM versions before 4.17.0-alpha.
CVE-2021-29415	The elliptic curve cryptography (ECC) hardware accelerator, part of the ARM® TrustZone® CryptoCell 310, contained in the NordicSemiconductor nRF52840 through 2 constant time ECDSA implemenation. This allows an adversary to recover the private ECC key used during an ECDSA operation.
CVE-2020-9451	An issue was discovered in Acronis True Image 2020 24.5.22510. anti_ransomware_service.exe keeps a log in a folder where unprivileged users have write permissior generated in a predictable pattern, allowing an unprivileged user to create a hardlink from a (not yet created) log file to anti_ransomware_service.exe. On reboot, this fo anti_ransomware_service to try to write its log into its own process, crashing in a SHARING VIOLATION. This crash occurs on every reboot.
CVE-2021-33425	A stored cross-site scripting (XSS) vulnerability was discovered in the Web Interface for OpenWRT LuCI version 19.07 which allows attackers to inject arbitrary Javascr Hostname via the Hostname Change operation.
CVE-2021-21660	Jenkins Markdown Formatter Plugin 0.1.0 and earlier does not sanitize crafted link target URLs, resulting in a stored cross-site scripting (XSS) vulnerability exploitable l ability to edit any description rendered using the configured markup formatter.

CVE Number	Description
CVE-2021-25934	In OpenNMS Horizon, versions opennms-18.0.0-1 through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundati meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.7-1 are vulnerable to Stored Cross-Site Scripting, since the function `createRequisitionedNode()` c validation checks on the input sent to the `node-label` parameter. Due to this flaw an attacker could inject an arbitrary script which will be stored in the database.
CVE-2021-23387	The package trailing-slash before 2.0.1 are vulnerable to Open Redirect via the use of trailing double slashes in the URL when accessing the vulnerable endpoint (such https://example.com//attacker.example/). The vulnerable code is in index.js::createTrailing(), as the web server uses relative URLs instead of absolute URLs.
CVE-2021-25935	In OpenNMS Horizon, versions opennms-17.0.0-1 through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundati meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.7-1 are vulnerable to Stored Cross-Site Scripting, since the function `add()` performs improper vali input sent to the `foreign-source` parameter. Due to this flaw an attacker could bypass the existing regex validation and inject an arbitrary script which will be stored in t
CVE-2021-33570	Postbird 0.8.4 allows stored XSS via the onerror attribute of an IMG element in any PostgreSQL database table. This can result in reading local files via vectors involvir and open of a file:/// URL, or discovering PostgreSQL passwords via vectors involving Window.localStorage and savedConnections.
CVE-2021-3313	Plone CMS until version 5.2.4 has a stored Cross-Site Scripting (XSS) vulnerability in the user fullname property and the file upload functionality. The user's input data i encoded when being echoed back to the user. This data can be interpreted as executable code by the browser and allows an attacker to execute JavaScript in the cont browser if the victim opens a vulnerable page containing an XSS payload.
CVE-2021-20374	IBM Maximo Asset Management 7.6.0 and 7.6.1 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the We intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195522.
CVE-2020-26555	Bluetooth legacy BR/EDR PIN code pairing in Bluetooth Core Specification 1.0B through 5.2 may permit an unauthenticated nearby device to spoof the BD_ADDR of th complete pairing without knowledge of the PIN.
CVE-2021-24308	The 'State' field of the Edit profile page of the LMS by LifterLMS – Online Course, Membership & Learning Management System Plugin for WordPress plugin before 4.2 sanitised when output in the About section of the profile page, leading to a stored Cross-Site Scripting issue. This could allow low privilege users (such as students) to e via an XSS attack when an admin will view their profile.
CVE-2021-24306	The Ultimate Member – User Profile, User Registration, Login & Membership Plugin WordPress plugin before 2.1.20 did not properly sanitise, validate or encode the qu generating a link to edit user's own profile, leading to an authenticated reflected Cross-Site Scripting issue. Knowledge of the targeted username is required to exploit th would then need to make the related logged in user open a malicious link.
CVE-2021-24302	The Hana Flv Player WordPress plugin through 3.1.3 is vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) vulnerability within the 'Default Skin' field.
CVE-2021-24301	The Hotjar Connecticator WordPress plugin through 1.1.1 is vulnerable to Stored Cross-Site Scripting (XSS) in the 'hotjar script' textarea. The request did include a CSI properly verified by the server and this vulnerability could only be exploited by administrator users.
CVE-2021-33508	Plone through 5.2.4 allows XSS via a full name that is mishandled during rendering of the ownership tab of a content item.
CVE-2021-33512	Plone through 5.2.4 allows stored XSS attacks (by a Contributor) by uploading an SVG or HTML document.
CVE-2021-20528	IBM Control Center 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intend potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198761.
CVE-2021-33513	Plone through 5.2.4 allows XSS via the inline_diff methods in Products.CMFDiffTool.
CVE-2021-29687	IBM Security Identity Manager 7.0.2 could allow a remote user to enumerate usernames due to a difference of responses from valid and invalid login attempts. IBM X-F
CVE-2021-27463	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the se is not properly invalidated, allowing an attacker to intercept the cookies and gain access to sensitive information.
CVE-2021-20529	IBM Control Center 6.2.0.0 could allow a user to obtain sensitive version information that could be used in further attacks against the system. IBM X-Force ID: 198763.
CVE-2021-30187	CODESYS V2 runtime system SP before 2.4.7.55 has Improper Neutralization of Special Elements used in an OS Command.

CVE Number	Description
CVE-2021-32640	ws is an open source WebSocket client and server library for Node.js. A specially crafted value of the `Sec-Websocket-Protocol` header can be used to significantly slo The vulnerability has been fixed in ws@7.4.6 (https://github.com/websockets/ws/commit/00c425ec77993773d823f018f64a5c44e17023ff). In vulnerable versions of ws, mitigated by reducing the maximum allowed length of the request headers using the [`--max-http-header-size=size`](https://nodejs.org/api/cli.html#cli_max_http_header the [`maxHeaderSize`](https://nodejs.org/api/http.html#http_http_createserver_options_requestlistener) options.
CVE-2017-17675	BMC Remedy Mid Tier 9.1SP3 is affected by log hijacking. Remote logging can be accessed by unauthenticated users, allowing for an attacker to hijack the system log include user names and HTTP data.
CVE-2021-29682	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. Tl be used in further attacks against the system. IBM X-Force ID: 199997
CVE-2021-22409	There is a denial of service vulnerability in some versions of ManageOne. There is a logic error in the implementation of a function of a module. When the service press a low probability that an exception may occur. Successful exploit may cause some services abnormal.
CVE-2021-21000	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the runtime.
CVE-2021-20428	IBM Security Guardium 11.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This infor in further attacks against the system. IBM X-Force ID: 196315.
CVE-2021-29681	IBM InfoSphere Information Server 11.7 could allow an attacker to obtain sensitive information by injecting parameters into an HTML query. This information could be u against the system. IBM X-Force ID: 199918.
CVE-2021-21552	Dell Wyse Windows Embedded System versions WIE10 LTSC 2019 and earlier contain an improper authorization vulnerability. A local authenticated malicious user wit potentially exploit this vulnerability to bypass the restricted environment and perform unauthorized actions on the affected system.
CVE-2021-21733	The management system of ZXCDN is impacted by the information leak vulnerability. Attackers can make further analysis according to the information returned by the obtain some sensitive information. This affects ZXCDN V7.01 all versions up to IAMV7.01.01.02.
CVE-2020-4839	IBM Host firmware for LC-class Systems is vulnerable to a stack based buffer overflow, caused by improper bounds checking. A remote privileged attacker could explo and cause a denial of service. IBM X-Force ID: 190037.
CVE-2021-29210	A remote dom xss, crlf injection vulnerability was discovered in HPE Integrated Lights-Out 4 (iLO 4); HPE SimpliVity 380 Gen9; HPE Integrated Lights-Out 5 (iLO 5) for HPE SimpliVity 380 Gen10; HPE SimpliVity 2600; HPE SimpliVity 380 Gen10 G; HPE SimpliVity 325; HPE SimpliVity 380 Gen10 H version(s): Prior to version 2.78.
CVE-2021-29209	A remote dom xss, crlf injection vulnerability was discovered in HPE Integrated Lights-Out 4 (iLO 4); HPE SimpliVity 380 Gen9; HPE Integrated Lights-Out 5 (iLO 5) for HPE SimpliVity 380 Gen10; HPE SimpliVity 2600; HPE SimpliVity 380 Gen10 G; HPE SimpliVity 325; HPE SimpliVity 380 Gen10 H version(s): Prior to version 2.78.
CVE-2021-29208	A remote dom xss, crlf injection vulnerability was discovered in HPE Integrated Lights-Out 4 (iLO 4); HPE SimpliVity 380 Gen9; HPE Integrated Lights-Out 5 (iLO 5) for HPE SimpliVity 380 Gen10; HPE SimpliVity 2600; HPE SimpliVity 380 Gen10 G; HPE SimpliVity 325; HPE SimpliVity 380 Gen10 H version(s): Prior to version 2.78.
CVE-2021-29211	A remote xss vulnerability was discovered in HPE Integrated Lights-Out 4 (iLO 4); HPE SimpliVity 380 Gen9; HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Serve 380 Gen10; HPE SimpliVity 2600; HPE SimpliVity 380 Gen10 G; HPE SimpliVity 325; HPE SimpliVity 380 Gen10 H version(s): Prior to version 2.78.
CVE-2021-29207	A remote xss vulnerability was discovered in HPE Integrated Lights-Out 4 (iLO 4); HPE SimpliVity 380 Gen9; HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Serve 380 Gen10; HPE SimpliVity 2600; HPE SimpliVity 380 Gen10 G; HPE SimpliVity 325; HPE SimpliVity 380 Gen10 H version(s): Prior to version 2.78.
CVE-2021-29206	A remote xss vulnerability was discovered in HPE Integrated Lights-Out 4 (iLO 4); HPE SimpliVity 380 Gen9; HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Serve 380 Gen10; HPE SimpliVity 2600; HPE SimpliVity 380 Gen10 G; HPE SimpliVity 325; HPE SimpliVity 380 Gen10 H version(s): Prior to version 2.78.
CVE-2021-29205	A remote xss vulnerability was discovered in HPE Integrated Lights-Out 4 (iLO 4); HPE SimpliVity 380 Gen9; HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Serve 380 Gen10; HPE SimpliVity 2600; HPE SimpliVity 380 Gen10 G; HPE SimpliVity 325; HPE SimpliVity 380 Gen10 H version(s): Prior to version 2.78.
CVE-2021-29204	A remote xss vulnerability was discovered in HPE Integrated Lights-Out 4 (iLO 4); HPE SimpliVity 380 Gen9; HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Serve 380 Gen10; HPE SimpliVity 2600; HPE SimpliVity 380 Gen10 G; HPE SimpliVity 325; HPE SimpliVity 380 Gen10 H version(s): Prior to version 2.78.
CVE-2021-1254	Multiple vulnerabilities in the web-based management interface of Cisco Finesse could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) a of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attac these vulnerabilities by injecting malicious code into the web-based management interface and persuading a user to click a malicious link. A successful exploit could all execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. An attacker needs valid administrator credentials to script code.

CVE Number	Description
CVE-2021-29201	A remote xss vulnerability was discovered in HPE Integrated Lights-Out 4 (iLO 4); HPE SimpliVity 380 Gen9; HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Serv 380 Gen10; HPE SimpliVity 2600; HPE SimpliVity 380 Gen10 G; HPE SimpliVity 325; HPE SimpliVity 380 Gen10 H version(s): Prior to version 2.78.
CVE-2021-25933	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-founda meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-Site Scripting, since the function `validateFormInput()` perform checks on the input sent to the `groupName` and `groupComment` parameters. Due to this flaw, an authenticated attacker could inject arbitrary script and trick other ac downloading malicious files which can cause severe damage to the organization using opennms.
CVE-2021-3536	A flaw was found in Wildfly in versions before 23.0.2.Final while creating a new role in domain mode via the admin console, it is possible to add a payload in the name f This affects Confidentiality and Integrity.
CVE-2021-33562	A reflected cross-site scripting (XSS) vulnerability in Shopizer before 2.17.0 allows remote attackers to inject arbitrary web script or HTML via the ref parameter to a pag product, e.g., a product/insert-product-name-here.html/ref= URL.
CVE-2021-33561	A stored cross-site scripting (XSS) vulnerability in Shopizer before 2.17.0 allows remote attackers to inject arbitrary web script or HTML via customer_name in various f administration. It is saved in the database. The code is executed for any user of store administration when information is fetched from the backend, e.g., in admin/custo
CVE-2021-24296	The WP Customer Reviews WordPress plugin before 3.5.6 did not sanitise some of its settings, allowing high privilege users such as administrators to set XSS payloac then be triggered in pages where reviews are enabled
CVE-2021-24332	The Autoptimize WordPress plugin before 2.8.4 was missing proper escaping and sanitisation in some of its settings, allowing high privilege users to set XSS payloads stored Cross-Site Scripting issues
CVE-2021-25929	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-founda meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-Site Scripting since there is no validation on the input being ser parameter in `noticeWizard` endpoint. Due to this flaw an authenticated attacker could inject arbitrary script and trick other admin users into downloading malicious files
CVE-2021-1553	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authe attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execut commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.
CVE-2021-1547	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authe attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execut commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.
CVE-2021-1552	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authe attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execut commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.
CVE-2021-1550	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authe attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execut commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.
CVE-2021-1549	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authe attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execut commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.
CVE-2021-1548	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authe attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execut commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.
CVE-2021-1358	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to redirect a user to an undesired web page. T due to improper input validation of the URL parameters in an HTTP request that is sent to an affected system. An attacker could exploit this vulnerability by persuading interface to click a crafted link. A successful exploit could allow the attacker to cause the interface to redirect the user to a specific, malicious URL. This type of vulnerat open redirect and is used in phishing attacks that get users to unknowingly visit malicious sites.

CVE Number	Description
CVE-2021-1551	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authe attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execut commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.
CVE-2021-1554	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authe attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execut commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.
CVE-2021-1555	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authe attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execut commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.
CVE-2021-27925	An issue was discovered in Couchbase Server 6.5.x and 6.6.x through 6.6.1. When using the View Engine and Auditing is enabled, a crash condition can (depending o cause an internal user with administrator privileges, @ns_server, to have its credentials leaked in cleartext in the ns_server.info.log file.
CVE-2021-1306	A vulnerability in the restricted shell of Cisco Evolved Programmable Network (EPN) Manager, Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure cou authenticated, local attacker to identify directories and write arbitrary files to the file system. This vulnerability is due to improper validation of parameters that are sent t within the restricted shell. An attacker could exploit this vulnerability by logging in to the device and issuing certain CLI commands. A successful exploit could allow the directories on the affected device and write arbitrary files to the file system on the affected device. To exploit this vulnerability, the attacker must be an authenticated sh
CVE-2021-32638	Github's CodeQL action is provided to run CodeQL-based code scanning on non-GitHub CI/CD systems and requires a GitHub access token to connect to a GitHub rep and its documentation previously suggested passing the GitHub token as a command-line parameter to the process instead of reading it from a file, standard input, or a variable. This approach made the token visible to other processes on the same machine, for example in the output of the `ps` command. If the CI system publicly expos for example by logging the output, then the GitHub access token can be exposed beyond the scope intended. Users of the CodeQL runner on 3rd-party systems, who a token via the `--github-auth` flag, are affected. This applies to both GitHub.com and GitHub Enterprise users. Users of the CodeQL Action on GitHub Actions are not aff auth` flag is now considered insecure and deprecated. The undocumented `--external-repository-token` flag has been removed. To securely provide a GitHub access to runner, users should **do one of the following instead**: Use the `--github-auth-stdin` flag and pass the token on the command line via standard input OR set the `GITH environment variable to contain the token, then call the command without passing in the token. The old flag remains present for backwards compatibility with existing w tries to specify an access token using the `--github-auth` flag, there is a deprecation warning printed to the terminal that directs the user to one of the above options. All releases codeql-bundle-20210304 onwards contain the patches. We recommend updating to a recent version of the CodeQL runner, storing a token in your CI system's mechanism, and passing the token to the CodeQL runner using `--github-auth-stdin` or the `GITHUB_TOKEN` environment variable. If still using the old flag, ensure tha such as from `ps`, is not persisted in CI logs.
CVE-2020-21056	Directory Traversal vulnerability exists in FusionPBX 4.5.7, which allows a remote malicious user to create folders via the folder variale to app\edit\foldernew.php.
CVE-2021-25930	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-founda meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to CSRF, due to no CSRF protection, and since there is no validation of an exis renaming a user. As a result, privileges of the renamed user are being overwritten by the old user and the old user is being deleted from the user list.
CVE-2020-4646	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5, 6.0.0.0 through 6.0.3.3, and 6.1.0.0 through 6.1.0.2 could allow an authenticated user to view pag have access to due to improper authorization control.
CVE-2020-10069	Zephyr Bluetooth unchecked packet data results in denial of service. Zephyr versions >= v1.14.2, >= v2.2.0 contain Improper Handling of Parameters (CWE-233). For m https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-f6vh-7v4x-8fjp
CVE-2021-33510	Plone through 5.2.4 allows remote authenticated managers to conduct SSRF attacks via an event ical URL, to read one line of a file.
CVE-2020-26558	Bluetooth LE and BR/EDR secure pairing in Bluetooth Core Specification 2.1 through 5.2 may permit a nearby man-in-the-middle attacker to identify the Passkey used Passkey authentication procedure) by reflection of the public key and the authentication evidence of the initiating device, potentially permitting this attacker to complete with the responding device using the correct Passkey for the pairing session. The attack methodology determines the Passkey value one bit at a time.
CVE-2020-13602	Remote Denial of Service in LwM2M do_write_op_tlv. Zephyr versions >= 1.14.2, >= 2.2.0 contain Improper Input Validation (CWE-20), Loop with Unreachable Exit Co (CWE-835). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-g9mg-fj58-6fqh
CVE-2020-10065	Missing Size Checks in Bluetooth HCI over SPI. Zephyr versions >= v1.14.2, >= v2.2.0 contain Improper Handling of Length Parameter Inconsistency (CWE-130). For m https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-hg2w-62p6-g67c
CVE-2020-4765	IBM Cloud Pak for Multicloud Management prior to 2.3 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 18890
CVE-2020-13599	Security problem with settings and littlefs. Zephyr versions >= 1.14.2, >= 2.3.0 contain Incorrect Default Permissions (CWE-276). For more information, see https://githu rtos/zephyr/security/advisories/GHSA-5qhg-j6wc-4f6q

CVE Number	Description
CVE-2020-10066	Incorrect Error Handling in Bluetooth HCI core. Zephyr versions >= v1.14.2, >= v2.2.0 contain NULL Pointer Dereference (CWE-476). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-gc66-xfrc-24qr
CVE-2021-32632	Pajbot is a Twitch chat bot. Pajbot versions prior to 1.52 are vulnerable to cross-site request forgery (CSRF). Hosters of the bot should upgrade to `v1.52` or `stable` to as a workaround, can add one modern dependency.