SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 January 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-2021-21245	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, AttachmentUploadServlet also saves user controlled data (`request.getInputStream()`) to a user specified location (`request.getHeader("File-Name")`). This issue may lead to arbitrary file upload which can be used to upload a WebShell to OneDev server. This issue is addressed in 4.0.3 by only allowing uploaded file to be in attachments folder. The webshell issue is not possible as OneDev never executes files in attachments folder.	10.0	More Details
CVE-2021-21242	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, there is a critical vulnerability which can lead to pre-auth remote code execution. AttachmentUploadServlet deserializes untrusted data from the `Attachment-Support` header. This Servlet does not enforce any authentication or authorization checks. This issue may lead to pre-auth remote code execution. This issue was fixed in 4.0.3 by removing AttachmentUploadServlet and not using deserialization	10.0	More Details
CVE-2021-21244	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, There is a vulnerability that enabled pre-auth server side template injection via Bean validation message tampering. Full details in the reference GHSA. This issue was fixed in 4.0.3 by disabling validation interpolation completely.	10.0	More Details
CVE-2021-21243	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, a Kubernetes REST endpoint exposes two methods that deserialize untrusted data from the request body. These endpoints do not enforce any authentication or authorization checks. This issue may lead to pre-auth RCE. This issue was fixed in 4.0.3 by not using deserialization at KubernetesResource side.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0211	An improper check for unusual or exceptional conditions in Juniper Networks Junos OS and Junos OS Evolved Routing Protocol Daemon (RPD) service allows an attacker to send a valid BGP FlowSpec message thereby causing an unexpected change in the route advertisements within the BGP FlowSpec domain leading to disruptions in network traffic causing a Denial of Service (DoS) condition. Continued receipt of these update messages will cause a sustained Denial of Service condition. This issue affects Juniper Networks: Junos OS: All versions prior to 17.3R3-S10 with the exceptions of 15.1X49-D240 on SRX Series and 15.1R7-S8 on EX Series; 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R2-S12, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R1-S3, 19.4R2-S3, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S3 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2. Junos OS Evolved: All versions prior to 20.3R1-S1-EVO, 20.3R2-EVO.	10.0	More Details
CVE-2020-29495	DELL EMC Avamar Server, versions 19.1, 19.2, 19.3, contain an OS Command Injection Vulnerability in Fitness Analyzer. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS with high privileges. This vulnerability is considered critical as it can be leveraged to completely compromise the vulnerable application as well as the underlying operating system. Dell recommends customers to upgrade at the earliest opportunity.	10.0	More Details
CVE-2020-29493	DELL EMC Avamar Server, versions 19.1, 19.2, 19.3, contain a SQL Injection Vulnerability in Fitness Analyzer. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the application's backend database, causing unauthorized read and write access to application data. Exploitation may lead to leakage or deletion of sensitive backup data; hence the severity is Critical. Dell EMC recommends customers to upgrade at the earliest opportunity.	10.0	More Details
CVE-2020-5633	Multiple NEC products (Express5800/T110j, Express5800/T110j-S, Express5800/T110j (2nd-Gen), Express5800/T110j-S (2nd-Gen), iStorage NS100Ti, and Express5800/GT110j) where Baseboard Management Controller (BMC) firmware Rev1.09 and earlier is applied allows remote attackers to bypass authentication and then obtain/modify BMC setting information, obtain monitoring information, or reboot/shut down the vulnerable product via unspecified vectors.	9.8	More Details
CVE-2020-29015	A blind SQL injection in the user interface of FortiWeb 6.3.0 through 6.3.7 and version before 6.2.4 may allow an unauthenticated, remote attacker to execute arbitrary SQL queries or commands by sending a request with a crafted Authorization header containing a malicious SQL statement.	9.8	More Details
CVE-2021-22851	HGiga EIP product contains SQL Injection vulnerability. Attackers can inject SQL commands into specific URL parameter (document management page) to obtain database schema and data.	9.8	More Details
CVE-2021-3177	Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely.	9.8	More Details
CVE-2021-25294	OpenCATS through 0.9.5-3 unsafely deserializes index.php?m=activity requests, leading to remote code execution. This occurs because lib/DataGrid.php calls unserialize for the parametersactivity:ActivityDataGrid parameter. The PHP object injection exploit chain can leverage an __destruct magic method in guzzlehttp.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24640	There is a vulnerability caused by insufficient input validation that allows for arbitrary command execution in a containerized environment within Airwave Glass before 1.3.3. Successful exploitation can lead to complete compromise of the underlying host operating system.	9.8	More Details
CVE-2020-24639	There is a vulnerability caused by unsafe Java deserialization that allows for arbitrary command execution in a containerized environment within Airwave Glass before 1.3.3. Successful exploitation can lead to complete compromise of the underlying host operating system.	9.8	More Details
CVE-2020-5685	UNIVERGE SV9500 series from V1 to V7and SV8500 series from S6 to S8 allows an attacker to execute arbitrary OS commands or cause a denial-of-service (DoS) condition by sending a specially crafted request to a specific URL.	9.8	More Details
CVE-2020-29016	A stack-based buffer overflow vulnerability in FortiWeb 6.3.0 through 6.3.5 and version before 6.2.4 may allow an unauthenticated, remote attacker to overwrite the content of the stack and potentially execute arbitrary code by sending a crafted request with a large certname.	9.8	More Details
CVE-2020-35929	In TinyCheck before commits 9fd360d and ea53de8, the installation script of the tool contained hard-coded credentials to the backend part of the tool. This information could be used by an attacker for unauthorized access to remote data.	9.8	More Details
CVE-2020-27488	Loxone Miniserver devices with firmware before 11.1 (aka 11.1.9.3) are unable to use an authentication method that is based on the "signature of the update package." Therefore, these devices (or attackers who are spoofing these devices) can continue to use an unauthenticated cloud service for an indeterminate time period (possibly forever). Once an individual device's firmware is updated, and authentication occurs once, the cloud service recategorizes the device so that authentication is subsequently always required, and spoofing cannot occur.	9.8	More Details
CVE-2020-9144	There is a heap overflow vulnerability in some Huawei smartphone, attackers can exploit this vulnerability to cause heap overflows due to improper restriction of operations within the bounds of a memory buffer.	9.8	More Details
CVE-2021-20617	Improper access control vulnerability in acmailer ver. 4.0.1 and earlier, and acmailer DB ver. 1.1.3 and earlier allows remote attackers to execute an arbitrary OS command, or gain an administrative privilege which may result in obtaining the sensitive information on the server via unspecified vectors.	9.8	More Details
CVE-2021-23899	OWASP json-sanitizer before 1.2.2 may emit closing SCRIPT tags and CDATA section delimiters for crafted input. This allows an attacker to inject arbitrary HTML or XML into embedding documents.	9.8	More Details
CVE-2020-27265	KEPServerEX: v6.0 to v6.9, ThingWorx Kepware Server: v6.8 and v6.9, ThingWorx Industrial Connectivity: All versions, OPC-Aggregator: All versions, Rockwell Automation KEPServer Enterprise, GE Digital Industrial Gateway Server: v7.68.804 and v7.66, Software Toolbox TOP Server: All 6.x versions are vulnerable to a stack-based buffer overflow. Opening a specifically crafted OPC UA message could allow an attacker to crash the server and remotely execute code.	9.8	More Details
CVE-2021-3028	git-big-picture before 1.0.0 mishandles ' characters in a branch name, leading to code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23653	An insecure unserialize vulnerability was discovered in ThinkAdmin versions 4.x through 6.x in app/admin/controller/api/Update.php and app/wechat/controller/api/Push.php, which may lead to arbitrary remote code execution.	9.8	More Details
CVE-2020-9140	There is a vulnerability with buffer access with incorrect length value in some Huawei Smartphone.Unauthorized users may trigger code execution when a buffer overflow occurs.	9.8	More Details
CVE-2021-20618	Privilege chaining vulnerability in acmailer ver. 4.0.2 and earlier, and acmailer DB ver. 1.1.4 and earlier allows remote attackers to bypass authentication and to gain an administrative privilege which may result in obtaining the sensitive information on the server via unspecified vectors.	9.8	More Details
CVE-2021-21249	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, there is an issue involving YAML parsing which can lead to post-auth remote code execution. In order to parse and process YAML files, OneDev uses SnakeYaml which by default (when not using `SafeConstructor`) allows the instantiation of arbitrary classes. We can leverage that to run arbitrary code by instantiating classes such as `javax.script.ScriptEngineManager` and using `URLClassLoader` to load the script engine provider, resulting in the instantiation of a user controlled class. For a full example refer to the referenced GHSA. This issue was addressed in 4.0.3 by only allowing certain known classes to be deserialized	9.6	More Details
CVE-2021-21248	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, there is a critical vulnerability involving the build endpoint parameters. InputSpec is used to define parameters of a Build spec. It does so by using dynamically generated Groovy classes. A user able to control job parameters can run arbitrary code on OneDev's server by injecting arbitrary Groovy code. The ultimate result is in the injection of a static constructor that will run arbitrary code. For a full example refer to the referenced GHSA. This issue was addressed in 4.0.3 by escaping special characters such as quote from user input.	9.6	More Details
CVE-2021-21247	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, the application's BasePage registers an AJAX event listener (`AbstractPostAjaxBehavior`) in all pages other than the login page. This listener decodes and deserializes the `data` query parameter. We can access this listener by submitting a POST request to any page. This issue may lead to `post-auth RCE` This endpoint is subject to authentication and, therefore, requires a valid user to carry on the attack. This issue was addressed in 4.0.3 by encrypting serialization payload with secrets only known to server.	9.6	More Details
CVE-2020-16045	Use after Free in Payments in Google Chrome on Android prior to 87.0.4280.66 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-2020-9145	There is an Out-of-bounds Write vulnerability in some Huawei smartphone. Successful exploitation of this vulnerability may cause out-of-bounds access to the physical memory.	9.1	More Details
CVE-2020-9139	There is a improper input validation vulnerability in some Huawei Smartphone.Successful exploit of this vulnerability can cause memory access errors and denial of service.	9.1	More Details
CVE-2020-9141	There is a improper privilege management vulnerability in some Huawei smartphone. Successful exploitation of this vulnerability can cause information disclosure and malfunctions due to insufficient verification of data authenticity.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9142	There is a heap base buffer overflow vulnerability in some Huawei smartphone.Successful exploitation of this vulnerability can cause heap overflow and memory overwriting when the system incorrectly processes the update file.	9.1	More Details
CVE-2020-27263	KEPServerEX: v6.0 to v6.9, ThingWorx Kepware Server: v6.8 and v6.9, ThingWorx Industrial Connectivity: All versions, OPC-Aggregator: All versions, Rockwell Automation KEPServer Enterprise, GE Digital Industrial Gateway Server: v7.68.804 and v7.66, Software Toolbox TOP Server: All 6.x versions, are vulnerable to a heap-based buffer overflow. Opening a specifically crafted OPC UA message could allow an attacker to crash the server and potentially leak data.	9.1	More Details
CVE-2020-27267	KEPServerEX v6.0 to v6.9, ThingWorx Kepware Server v6.8 and v6.9, ThingWorx Industrial Connectivity (all versions), OPC-Aggregator (all versions), Rockwell Automation KEPServer Enterprise, GE Digital Industrial Gateway Server v7.68.804 and v7.66, and Software Toolbox TOP Server all 6.x versions, are vulnerable to a heap-based buffer overflow. Opening a specifically crafted OPC UA message could allow an attacker to crash the server and potentially leak data.	9.1	More Details
CVE-2021-25323	The default setting of MISP 2.4.136 did not enable the requirements (aka require_password_confirmation) to provide the previous password when changing a password.	9.1	More Details
CVE-2021-23926	The XML parsers used by XMLBeans up to version 2.6.0 did not set the properties needed to protect the user from malicious XML input. Vulnerabilities include possibilities for XML Entity Expansion attacks. Affects XMLBeans up to and including v2.6.0.	9.1	More Details
CVE-2020-35128	Mautic before 3.2.4 is affected by stored XSS. An attacker with permission to manage companies, an application feature, could attack other users, including administrators. For example, by loading an externally crafted JavaScript file, an attacker could eventually perform actions as the target user. These actions include changing the user passwords, altering user or email addresses, or adding a new administrator to the system.	9.0	More Details
CVE-2020-35129	Mautic before 3.2.4 is affected by stored XSS. An attacker with access to Social Monitoring, an application feature, could attack other users, including administrators. For example, an attacker could load an externally drafted JavaScript file that would allow them to eventually perform actions on the target user's behalf, including changing the user's password or email address or changing the attacker's user role from a low-privileged user to an administrator account.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2021-0208	An improper input validation vulnerability in the Routing Protocol Daemon (RPD) service of Juniper Networks Junos OS allows an attacker to send a malformed RSVP packet when bidirectional LSPs are in use, which when received by an egress router crashes the RPD causing a Denial of Service (DoS) condition. Continued receipt of the packet will sustain the Denial of Service. This issue affects: Juniper Networks Junos OS: All versions prior to 17.3R3-S10 except 15.1X49-D240 for SRX series; 17.4 versions prior to 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S4; 18.3 versions prior to 18.3R3-S2; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S2; 19.1 versions prior to 19.1R1-S5, 19.1R3-S3; 19.2 versions prior to 19.2R3; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R2-S2, 19.4R3-S1; 20.1 versions prior to 20.1R1-S4, 20.1R2; 15.1X49 versions prior to 15.1X49-D240 on SRX Series. Juniper Networks Junos OS Evolved: 19.3 versions prior to 19.3R2-S5-EVO; 19.4 versions prior to 19.4R2-S2-EVO; 20.1 versions prior to 20.1R1-S4-EVO.	8.8	More Details
CVE-2020-6776	A vulnerability in the web-based management interface of Bosch PRAESIDEO until and including version 4.41 and Bosch PRAESENSA until and including version 1.10 allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (Cross-Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or submitting a malicious form. A successful exploit allows the attacker to perform arbitrary actions with the privileges of the victim, e.g. creating and modifying user accounts, changing system configuration settings and cause DoS conditions. Note: For Bosch PRAESIDEO 4.31 and newer and Bosch PRAESENSA in all versions, the confidentiality impact is considered low because user credentials are not shown in the web interface.	8.8	More Details
CVE-2020-23342	A CSRF vulnerability exists in Anchor CMS 0.12.7 anchor/views/users/edit.php that can change the Delete admin users.	8.8	More Details
CVE-2021-1144	A vulnerability in Cisco Connected Mobile Experiences (CMX) could allow a remote, authenticated attacker without administrative privileges to alter the password of any user on an affected system. The vulnerability is due to incorrect handling of authorization checks for changing a password. An authenticated attacker without administrative privileges could exploit this vulnerability by sending a modified HTTP request to an affected device. A successful exploit could allow the attacker to alter the passwords of any user on the system, including an administrative user, and then impersonate that user.	8.8	More Details
CVE-2020-27733	Zoho ManageEngine Applications Manager before 14 build 14880 allows an authenticated SQL Injection via a crafted Alarmview request.	8.8	More Details
CVE-2020-27220	The Eclipse Hono AMQP and MQTT protocol adapters do not check whether an authenticated gateway device is authorized to receive command & control messages when it has subscribed only to commands for a specific device. The missing check involves verifying that the command target device is configured giving permission for the gateway device to act on its behalf. This means an authenticated device of a certain tenant, notably also a non-gateway device acting like a gateway, may receive command & control messages targeted at a different device of the same tenant without corresponding permissions getting checked.	8.8	More Details
CVE-2020-6572	Use after free in Media in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to execute arbitrary code via a crafted HTML page.	8.8	More Details
CVE-2021-22852	HGiga EIP product contains SQL Injection vulnerability. Attackers can inject SQL commands into specific URL parameter (online registration) to obtain database schema and data.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29018	A format string vulnerability in FortiWeb 6.3.0 through 6.3.5 may allow an authenticated, remote attacker to read the content of memory and retrieve sensitive data via the redir parameter.	8.8	More Details
CVE-2020-29017	An OS command injection vulnerability in FortiDeceptor 3.1.0, 3.0.1, 3.0.0 may allow a remote authenticated attacker to execute arbitrary commands on the system by exploiting a command injection vulnerability on the Customization page.	8.8	More Details
CVE-2020-27264	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, the communication protocol of the insulin pump and its AnyDana-i and AnyDana-A mobile applications use deterministic keys, which allows unauthenticated, physically proximate attackers to brute-force the keys via Bluetooth Low Energy.	8.8	More Details
CVE-2020-29494	Dell EMC Avamar Server, versions 19.1, 19.2, 19.3, contain a Path Traversal Vulnerability in PDM. A remote user could potentially exploit this vulnerability, to gain unauthorized write access to the arbitrary files stored on the server filesystem, causing deletion of arbitrary files.	8.7	More Details
CVE-2021-0203	On Juniper Networks EX and QFX5K Series platforms configured with Redundant Trunk Group (RTG), Storm Control profile applied on the RTG interface might not take affect when it reaches the threshold condition. Storm Control enables the device to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. Note: this issue does not affect EX2200, EX3300, EX4200, and EX9200 Series. This issue affects Juniper Networks Junos OS on EX Series and QFX5K Series: 15.1 versions prior to 15.1R7-S7; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S5, 18.4R3-S3; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2.	8.6	More Details
CVE-2021-21009	Adobe Campaign Classic Gold Standard 10 (and earlier), 20.3.1 (and earlier), 20.2.3 (and earlier), 20.1.3 (and earlier), 19.2.3 (and earlier) and 19.1.7 (and earlier) are affected by a server-side request forgery (SSRF) vulnerability. Successful exploitation could allow an attacker to use the Campaign instance to issue unauthorized requests to internal or external resources.	8.6	More Details
CVE-2021-21246	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, the REST UserResource endpoint performs a security check to make sure that only administrators can list user details. However for the `/users/{id}` endpoint there are no security checks enforced so it is possible to retrieve arbitrary user details including their Access Tokens! These access tokens can be used to access the API or clone code in the build spec via the HTTP(S) protocol. It has permissions to all projects accessible by the user account. This issue may lead to `Sensitive data leak` and leak the Access Token which can be used to impersonate the administrator or any other users. This issue was addressed in 4.0.3 by removing user info from restful api.	8.6	More Details
CVE-2021-21006	Adobe Photoshop version 22.1 (and earlier) is affected by a heap buffer overflow vulnerability when handling a specially crafted font file. Successful exploitation could lead to arbitrary code execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	8.6	More Details
CVE-2021-3139	In Open-iSCSI tcmu-runner 1.3.x, 1.4.x, and 1.5.x through 1.5.2, xcopy_locate_udev in tcmur_cmd_handler.c lacks a check for transport-layer restrictions, allowing remote attackers to read or write files via directory traversal in an XCOPY request. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. NOTE: relative to CVE-2020-28374, this is a similar mistake in a different algorithm.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21013	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to an insecure direct object vulnerability (IDOR) in the customer API module. Successful exploitation could lead to sensitive information disclosure and update arbitrary information on another user's account.	8.1	More Details
CVE-2019-4702	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.	8.1	More Details
CVE-2020-28374	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.	8.1	More Details
CVE-2021-22498	XML External Entity Injection vulnerability in Micro Focus Application Lifecycle Management (Previously known as Quality Center) product. The vulnerability affects versions 12.x, 12.60 Patch 5 and earlier, 15.0.1 Patch 2 and earlier and 15.5. The vulnerability could be exploited to allow an XML External Entity Injection.	8.1	More Details
CVE-2021-20190	A flaw was found in jackson-databind before 2.9.10.7. FasterXML mishandles the interaction between serialization gadgets and typing. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.1	More Details
CVE-2021-21605	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows users with Agent/Configure permission to choose agent names that cause Jenkins to override the global `config.xml` file.	8.0	More Details
CVE-2021-3182	D-Link DCS-5220 devices have a buffer overflow. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	8.0	More Details
CVE-2021-21604	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows attackers with permission to create or configure various objects to inject crafted content into Old Data Monitor that results in the instantiation of potentially unsafe objects once discarded by an administrator.	8.0	More Details
CVE-2021-20616	Untrusted search path vulnerability in the installer of SKYSEA Client View Ver.1.020.05b to Ver.16.001.01g allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	7.8	More Details
CVE-2021-0218	A command injection vulnerability in the license-check daemon of Juniper Networks Junos OS that may allow a locally authenticated attacker with low privileges to execute commands with root privilege. license-check is a daemon used to manage licenses in Junos OS. To update licenses, a user executes the command 'request system license update' via the CLI. An attacker with access to this CLI command may be able to exploit the vulnerability. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0223	A local privilege escalation vulnerability in telnetd.real of Juniper Networks Junos OS may allow a locally authenticated shell user to escalate privileges and execute arbitrary commands as root. telnetd.real is shipped with setuid permissions enabled and is owned by the root user, allowing local users to run telnetd.real with root privileges. This issue affects Juniper Networks Junos OS: all versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R2-S4, 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R2.	7.8	More Details
CVE-2020-14409	SDL (Simple DirectMedia Layer) through 2.0.12 has an Integer Overflow (and resultant SDL_memcpy heap corruption) in SDL_BlitCopy in video/SDL_blit_copy.c via a crafted .BMP file.	7.8	More Details
CVE-2021-3162	Docker Desktop Community before 2.5.0.0 on macOS mishandles certificate checking, leading to local privilege escalation.	7.8	More Details
CVE-2021-0204	A sensitive information disclosure vulnerability in delta-export configuration utility (dexp) of Juniper Networks Junos OS may allow a locally authenticated shell user the ability to create and read database files generated by the dexp utility, including password hashes of local users. Since dexp is shipped with setuid permissions enabled and is owned by the root user, this vulnerability may allow a local privileged user the ability to run dexp with root privileges and access sensitive information in the dexp database. This issue affects Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S8; 15.1X49 versions prior to 15.1X49-D230; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D34; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R1-S5, 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3-S1; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2.	7.8	More Details
CVE-2021-25174	An issue was discovered in Open Design Alliance Drawings SDK before 2021.12. A memory corruption vulnerability exists when reading malformed DGN files. It can allow attackers to cause a crash, potentially enabling denial of service (Crash, Exit, or Restart).	7.8	More Details
CVE-2021-25173	An issue was discovered in Open Design Alliance Drawings SDK before 2021.12. A memory allocation with excessive size vulnerability exists when reading malformed DGN files, which allows attackers to cause a crash, potentially enabling denial of service (crash, exit, or restart).	7.8	More Details
CVE-2021-25175	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A Type Conversion issue exists when rendering malformed .DXF and .DWG files. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart).	7.8	More Details
CVE-2021-25176	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A NULL pointer dereference exists when rendering malformed .DXF and .DWG files. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart).	7.8	More Details
CVE-2021-25177	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A Type Confusion issue exists when rendering malformed .DXF and .DWG files. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35686	The SECOMN service in Sound Research DCHU model software component modules (APO) through 2.0.9.17, delivered on HP Windows 10 computers, may allow escalation of privilege via a fake DLL. (As a resolution, Windows Update is being submitted for all affected products to update to 2.0.9.18 or later.)	7.8	More Details
CVE-2021-25178	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A stack-based buffer overflow vulnerability exists when the recover operation is run with malformed .DXF and .DWG files. This can allow attackers to cause a crash potentially enabling a denial of service attack (Crash, Exit, or Restart) or possible code execution.	7.8	More Details
CVE-2021-1237	A vulnerability in the Network Access Manager and Web Security Agent components of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL injection attack. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of resources that are loaded by the application at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path in the system which, in turn, causes a malicious DLL file to be loaded when the application starts. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with SYSTEM privileges.	7.8	More Details
CVE-2021-21251	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3 there is a critical "zip slip" vulnerability. This issue may lead to arbitrary file write. The KubernetesResource REST endpoint untars user controlled data from the request body using TarUtils. TarUtils is a custom library method leveraging Apache Commons Compress. During the untar process, there are no checks in place to prevent an untarred file from traversing the file system and overriding an existing file. For a successful exploitation, the attacker requires a valid __JobToken__ which may not be possible to get without using any of the other reported vulnerabilities. But this should be considered a vulnerability in `io.onedev.commons.utils.TarUtils` since it lives in a different artifact and can affect other projects using it. This issue was addressed in 4.0.3 by validating paths in tar archive to only allow them to be in specified folder when extracted.	7.7	More Details
CVE-2021-21250	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, there is a critical vulnerability which may lead to arbitrary file read. When BuildSpec is provided in XML format, the spec is processed by XmlBuildSpecMigrator.migrate(buildSpecString); which processes the XML document without preventing the expansion of external entities. These entities can be configured to read arbitrary files from the file system and dump their contents in the final XML document to be migrated. If the files are dumped in properties included in the YAML file, it will be possible for an attacker to read them. If not, it is possible for an attacker to exfiltrate the contents of these files Out Of Band. This issue was addressed in 4.0.3 by ignoring ENTITY instructions in xml file.	7.7	More Details
CVE-2020-35749	Directory traversal vulnerability in class-simple_job_board_resume_download_handler.php in the Simple Board Job plugin 2.9.3 and earlier for WordPress allows remote attackers to read arbitrary files via the sjb_file parameter to wp-admin/post.php.	7.7	More Details
CVE-2020-5686	Incorrect implementation of authentication algorithm issue in UNIVERGE SV9500 series from V1 to V7and SV8500 series from S6 to S8 allows an attacker to access the remote system maintenance feature and obtain the information by sending a specially crafted request to a specific URL.	7.5	More Details
CVE-2020-28478	This affects the package gsap before 3.6.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0202	On Juniper Networks MX Series and EX9200 Series platforms with Trio-based MPC (Modular Port Concentrator) where Integrated Routing and Bridging (IRB) interface is configured and it is mapped to a VPLS instance or a Bridge-Domain, certain network events at Customer Edge (CE) device may cause memory leak in the MPC which can cause an out of memory and MPC restarts. When this issue occurs, there will be temporary traffic interruption until the MPC is restored. An administrator can use the following CLI command to monitor the status of memory usage level of the MPC: user@device> show system resource-monitor fpc FPC Resource Usage Summary Free Heap Mem Watermark : 20 % Free NH Mem Watermark : 20 % Free Filter Mem Watermark : 20 % * - Watermark reached Slot # % Heap Free RTT Average RTT 1 87 PFE # % ENCAP mem Free % NH mem Free % FW mem Free 0 NA 88 99 1 NA 89 99 When the issue is occurring, the value of “% NH mem Free” will go down until the MPC restarts. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX Series, EX9200 Series: 17.3R3-S8; 17.4R3-S2; 18.2R3-S4, 18.2R3-S5; 18.3R3-S2, 18.3R3-S3; 18.4 versions starting from 18.4R3-S1 and later versions prior to 18.4R3-S6; 19.2 versions starting from 19.2R2 and later versions prior to 19.2R3-S1; 19.4 versions starting from 19.4R2 and later versions prior to 19.4R2-S3, 19.4R3; 20.2 versions starting from 20.2R1 and later versions prior to 20.2R1-S3, 20.2R2. This issue does not affect Juniper Networks Junos OS: 18.1, 19.1, 19.3, 20.1.	7.5	More Details
CVE-2020-35733	An issue was discovered in Erlang/OTP before 23.2.2. The ssl application 10.2 accepts and trusts an invalid X.509 certificate chain to a trusted root Certification Authority.	7.5	More Details
CVE-2021-1223	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.	7.5	More Details
CVE-2020-14101	The data collection SDK of the router web management interface caused the leakage of the token. This affects Xiaomi router AX1800rom version < 1.0.336 and Xiaomi route RM1800 root version < 1.0.26.	7.5	More Details
CVE-2020-14097	Wrong nginx configuration, causing specific paths to be downloaded without authorization. This affects Xiaomi router AX6 ROM version < 1.0.18.	7.5	More Details
CVE-2020-14098	The login verification can be bypassed by using the problem that the time is not synchronized after the router restarts. This affects Xiaomi router AX1800rom version < 1.0.336 and Xiaomi route RM1800 root version < 1.0.26.	7.5	More Details
CVE-2021-3138	In Discourse 2.7.0 through beta1, a rate-limit bypass leads to a bypass of the 2FA requirement for certain forms.	7.5	More Details
CVE-2020-26732	SKYWORTH GN542VF Hardware Version 2.0 and Software Version 2.0.0.16 does not set the Secure flag for the session cookie in an HTTPS session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an HTTP session.	7.5	More Details
CVE-2020-4881	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information, caused by the lack of server hostname verification for SSL/TLS communication. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 190851.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3131	The Web server in 1C:Enterprise 8 before 8.3.17.1851 sends base64 encoded credentials in the creds URL parameter.	7.5	More Details
CVE-2021-0206	A NULL Pointer Dereference vulnerability in Juniper Networks Junos OS allows an attacker to send a specific packet causing the packet forwarding engine (PFE) to crash and restart, resulting in a Denial of Service (DoS). By continuously sending these specific packets, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue only affects Juniper Networks NFX Series, SRX Series platforms when SSL Proxy is configured. This issue affects Juniper Networks Junos OS on NFX Series and SRX Series: 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S1; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S2, 19.2R2; 19.3 versions prior to 19.3R2. This issue does not affect Juniper Networks Junos OS versions on NFX Series and SRX Series prior to 18.3R1.	7.5	More Details
CVE-2021-3113	Netsia SEBA+ through 0.16.1 build 70-e669dcd7 allows remote attackers to discover session cookies via a direct /session/list/allActiveSession request. For example, the attacker can discover the admin's cookie if the admin account happens to be logged in when the allActiveSession request occurs, and can then use that cookie immediately for admin access,	7.5	More Details
CVE-2020-28477	This affects all versions of package immer.	7.5	More Details
CVE-2021-0207	An improper interpretation conflict of certain data between certain software components within the Juniper Networks Junos OS devices does not allow certain traffic to pass through the device upon receipt from an ingress interface filtering certain specific types of traffic which is then being redirected to an egress interface on a different VLAN. This causes a Denial of Service (DoS) to those clients sending these particular types of traffic. Such traffic being sent by a client may appear genuine, but is non-standard in nature and should be considered as potentially malicious, and can be targeted to the device, or destined through it for the issue to occur. This issues affects IPv4 and IPv6 traffic. An indicator of compromise may be found by checking log files. You may find that traffic on the input interface has 100% of traffic flowing into the device, yet the egress interface shows 0 pps leaving the device. For example: [show interfaces "interface" statistics detail] Output between two interfaces would reveal something similar to: Ingress, first interface: ---------- Interface Link Input packets (pps) Output packets (pps) et-0/0/0 Up 9999999999 (9999) 1 (0) ---------- Egress, second interface: ---------- Interface Link Input packets (pps) Output packets (pps) et-0/0/1 Up 0 (0) 9999999999 (0) ---------- Dropped packets will not show up in DDoS monitoring/protection counters as issue is not caused by anti-DDoS protection mechanisms. This issue affects: Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S7 on NFX250, QFX5K Series, EX4600; 17.4 versions prior to 17.4R2-S11, 17.4R3-S3 on NFX250, QFX5K Series, EX4600; 18.1 versions prior to 18.1R3-S9 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4600; 18.2 versions prior to 18.2R3-S3 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600; 18.3 versions prior to 18.3R3-S1 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series; 19.2 versions prior to 19.2R1-S5, 19.2R2 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series; 19.3 versions prior to 19.3R2-S3, 19.3R3 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series; 19.4 versions prior to 19.4R1-S2, 19.4R2 on NFX250, NFX350, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series. This issue does not affect Junos OS releases prior to 17.2R2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23900	OWASP json-sanitizer before 1.2.2 can output invalid JSON or throw an undeclared exception for crafted input. This may lead to denial of service if the application is not prepared to handle these situations.	7.5	More Details
CVE-2020-36193	Tar.php in Archive_Tar through 1.4.11 allows write operations with Directory Traversal due to inadequate checking of symbolic links, a related issue to CVE-2020-28948.	7.5	More Details
CVE-2019-4160	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 158577.	7.5	More Details
CVE-2020-4594	IBM Security Guardium Insights 2.0.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 184800.	7.5	More Details
CVE-2020-4596	IBM Security Guardium Insights 2.0.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 184812.	7.5	More Details
CVE-2021-3166	An issue was discovered on ASUS DSL-N14U-B1 1.1.2.3_805 devices. An attacker can upload arbitrary file content as a firmware update when the filename Settings_DSL-N14U-B1.trx is used. Once this file is loaded, shutdown measures on a wide range of services are triggered as if it were a real update, resulting in a persistent outage of those services.	7.5	More Details
CVE-2020-4595	IBM Security Guardium Insights 2.0.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 184819.	7.5	More Details
CVE-2020-24641	In Aruba AirWave Glass before 1.3.3, there is a Server-Side Request Forgery vulnerability through an unauthenticated endpoint that if successfully exploited can result in disclosure of sensitive information. This can be used to perform an authentication bypass and ultimately gain administrative access on the web administrative interface.	7.5	More Details
CVE-2021-3183	Files.com Fat Client 3.3.6 allows authentication bypass because the client continues to have access after a logout and a removal of a login profile.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0217	A vulnerability in processing of certain DHCP packets from adjacent clients on EX Series and QFX Series switches running Juniper Networks Junos OS with DHCP local/relay server configured may lead to exhaustion of DMA memory causing a Denial of Service (DoS). Over time, exploitation of this vulnerability may cause traffic to stop being forwarded, or to crashing of the fxpc process. When Packet DMA heap utilization reaches 99%, the system will become unstable. Packet DMA heap utilization can be monitored through the following command: user@junos# request pfe execute target fpc0 timeout 30 command "show heap" ID Base Total(b) Free(b) Used(b) % Name -- ---------- ---------- ---------- ---------- --- ---------- 0 213301a8 536870488 387228840 149641648 27 Kernel 1 91800000 8388608 3735120 4653488 55 DMA 2 92000000 75497472 74452192 1045280 1 PKT DMA DESC 3 d330000 335544320 257091400 78452920 23 Bcm_sdk 4 96800000 184549376 2408 184546968 99 Packet DMA <--- 5 903fffe0 20971504 20971504 0 0 Blob An indication of the issue occurring may be observed through the following log messages: Dec 10 08:07:00.124 2020 hostname fpc0 brcm_pkt_buf_alloc:523 (buf alloc) failed allocating packet buffer Dec 10 08:07:00.126 2020 hostname fpc0 (buf alloc) failed allocating packet buffer Dec 10 08:07:00.128 2020 hostname fpc0 brcm_pkt_buf_alloc:523 (buf alloc) failed allocating packet buffer Dec 10 08:07:00.130 2020 hostnameC fpc0 (buf alloc) failed allocating packet buffer This issue affects Juniper Networks Junos OS on EX Series and QFX Series: 17.4R3 versions prior to 17.4R3-S3; 18.1R3 versions between 18.1R3-S6 and 18.1R3-S11; 18.2R3 versions prior to 18.2R3-S6; 18.3R3 versions prior to 18.3R3-S4; 18.4R2 versions prior to 18.4R2-S5; 18.4R3 versions prior to 18.4R3-S6; 19.1 versions between 19.1R2 and 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2. Junos OS versions prior to 17.4R3 are unaffected by this vulnerability.	7.4	More Details
CVE-2021-0222	A vulnerability in Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) to the device by sending certain crafted protocol packets from an adjacent device with invalid payloads to the device. These crafted packets, which should be discarded, are instead replicated and sent to the RE. Over time, a Denial of Service (DoS) occurs. Continued receipt of these crafted protocol packets will cause an extended Denial of Service (DoS) condition, which may cause wider traffic impact due to protocol flapping. An indication of compromise is to check "monitor interface traffic" on the ingress and egress port packet counts. For each ingress packet, two duplicate packets are seen on egress. This issue can be triggered by IPv4 and IPv6 packets. This issue affects all traffic through the device. This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D53 on EX4300, QFX3500, QFX5100, EX4600; 15.1 versions prior to 15.1R7-S6 on EX4300, QFX3500, QFX5100, EX4600; 16.1 versions prior to 16.1R7-S7 on EX4300, QFX5100, EX4600; 17.1 versions prior to 17.1R2-S11 on EX4300, QFX5100, EX4600; 17.1 versions prior to 117.1R3-S2 on EX4300; 17.2 versions prior to 17.2R1-S9 on EX4300; 17.2 versions prior to 17.2R3-S3 on EX4300, QFX5100, EX4600, QFX5110, QFX5200; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on EX4300, QFX5100, EX4600, QFX5110, QFX5200; 17.4 versions prior to 17.4R2-S9, 17.4R3 on EX4300, QFX5100, EX4600, QFX5110, QFX5200; 18.1 versions prior to 18.1R3-S9 on EX4300, QFX5100, EX4600, QFX5110, QFX5200, QFX5210, EX2300, EX3400; 18.2 versions prior to 18.2R2-S7 on EX4300; 18.2 versions prior to 18.2R3-S3 on EX4300, QFX5100, EX4600, QFX5110, QFX5200, QFX5210, EX2300, EX3400; 18.3 versions prior to 18.3R2-S3, on EX4300; 18.3 versions prior to 18.3R1-S7, 18.3R3-S1 on EX4300, QFX5100, EX4600, QFX5110, QFX5200, QFX5210, QFX5120, EX4650, EX2300, EX3400; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on EX4300, QFX5100, EX4600, QFX5110, QFX5200, QFX5210, QFX5120, EX4650, EX2300, EX3400; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on EX4300, QFX5100, EX4600, QFX5110, QFX5200, QFX5210, QFX5120, EX4650, EX2300, EX3400; 19.2 versions prior to 19.2R1-S4, 19.2R2 on EX4300; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX5100, EX4600, QFX5110, QFX5200, QFX5210, QFX5120, EX4650, EX2300, EX3400; 19.3 versions prior to 19.3R2-S1, 19.3R3 on EX4300; 19.3 versions prior to 19.3R1-S1, 19.3R2, 19.3R3 on QFX5100, EX4600, QFX5110, QFX5200, QFX5210, QFX5120, EX4650, EX2300, EX3400;	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28480	The package jointjs before 3.3.0 are vulnerable to Prototype Pollution via util.setByPath (https://resources.jointjs.com/docs/jointjs/v3.2/joint.htmlutil.setByPath). The path used the access the object's key and set the value is not properly sanitized, leading to a Prototype Pollution.	7.3	More Details
CVE-2020-28472	This affects the package @aws-sdk/shared-ini-file-loader before 1.0.0-rc.9; the package aws-sdk before 2.814.0. If an attacker submits a malicious INI file to an application that parses it with loadSharedConfigFiles , they will pollute the prototype on the application. This can be exploited further depending on the context.	7.3	More Details
CVE-2021-22171	Insufficient validation of authentication parameters in GitLab Pages for GitLab 11.5+ allows an attacker to steal a victim's API token if they click on a maliciously crafted link	7.3	More Details
CVE-2020-28470	This affects the package @scullyio/scully before 1.0.9. The transfer state is serialised with the JSON.stringify() function and then written into the HTML page.	7.3	More Details
CVE-2021-21261	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. A bug was discovered in the `flatpak-portal` service that can allow sandboxed applications to execute arbitrary code on the host system (a sandbox escape). This sandbox-escape bug is present in versions from 0.11.4 and before fixed versions 1.8.5 and 1.10.0. The Flatpak portal D-Bus service (`flatpak-portal`, also known by its D-Bus service name `org.freedesktop.portal.Flatpak`) allows apps in a Flatpak sandbox to launch their own subprocesses in a new sandbox instance, either with the same security settings as the caller or with more restrictive security settings. For example, this is used in Flatpak-packaged web browsers such as Chromium to launch subprocesses that will process untrusted web content, and give those subprocesses a more restrictive sandbox than the browser itself. In vulnerable versions, the Flatpak portal service passes caller-specified environment variables to non-sandboxed processes on the host system, and in particular to the `flatpak run` command that is used to launch the new sandbox instance. A malicious or compromised Flatpak app could set environment variables that are trusted by the `flatpak run` command, and use them to execute arbitrary code that is not in a sandbox. As a workaround, this vulnerability can be mitigated by preventing the `flatpak-portal` service from starting, but that mitigation will prevent many Flatpak apps from working correctly. This is fixed in versions 1.8.5 and 1.10.0.	7.3	More Details
CVE-2021-1199	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1202	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1210	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1200	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1201	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1198	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1203	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1204	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1205	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1206	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1207	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1208	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1209	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1307	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1211	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1212	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1213	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1214	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1215	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1216	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1217	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14102	There is command injection when ddns processes the hostname, which causes the administrator user to obtain the root privilege of the router. This affects Xiaomi router AX1800rom version < 1.0.336 and Xiaomi route RM1800 root version < 1.0.26.	7.2	More Details
CVE-2021-21263	Laravel is a web application framework. Versions of Laravel before 6.20.11, 7.30.2 and 8.22.1 contain a query binding exploitation. This same exploit applies to the illuminate/database package which is used by Laravel. If a request is crafted where a field that is normally a non-array value is an array, and that input is not validated or cast to its expected type before being passed to the query builder, an unexpected number of query bindings can be added to the query. In some situations, this will simply lead to no results being returned by the query builder; however, it is possible certain queries could be affected in a way that causes the query to return unexpected results.	7.2	More Details
CVE-2020-24638	Multiple authenticated remote command executions are possible in Airwave Glass before 1.3.3 via the glassadmin cli. These allow for a user with glassadmin privileges to execute arbitrary code as root on the underlying host operating system.	7.2	More Details
CVE-2021-21237	Git LFS is a command line extension for managing large files with Git. On Windows, if Git LFS operates on a malicious repository with a git.bat or git.exe file in the current directory, that program would be executed, permitting the attacker to execute arbitrary code. This does not affect Unix systems. This is the result of an incomplete fix for CVE-2020-27955. This issue occurs because on Windows, Go includes (and prefers) the current directory when the name of a command run does not contain a directory separator. Other than avoiding untrusted repositories or using a different operating system, there is no workaround. This is fixed in v2.13.2.	7.2	More Details
CVE-2021-1196	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1197	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1360	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1195	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1172	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1146	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1149	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1171	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1150	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1194	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1189	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2020-35578	An issue was discovered in the Manage Plugins page in Nagios XI before 5.8.0. Because the line-ending conversion feature is mishandled during a plugin upload, a remote, authenticated admin user can execute operating-system commands.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1159	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2020-26262	Coturn is free open source implementation of TURN and STUN Server. Coturn before version 4.5.2 by default does not allow peers to connect and relay packets to loopback addresses in the range of `127.x.x.x`. However, it was observed that when sending a `CONNECT` request with the `XOR-PEER-ADDRESS` value of `0.0.0.0`, a successful response was received and subsequently, `CONNECTIONBIND` also received a successful response. Coturn then is able to relay packets to the loopback interface. Additionally, when coturn is listening on IPv6, which is default, the loopback interface can also be reached by making use of either `[::1]` or `[::]` as the peer address. By using the address `0.0.0.0` as the peer address, a malicious user will be able to relay packets to the loopback interface, unless `--denied-peer-ip=0.0.0.0` (or similar) has been specified. Since the default configuration implies that loopback peers are not allowed, coturn administrators may choose to not set the `denied-peer-ip` setting. The issue patched in version 4.5.2. As a workaround the addresses in the address block `0.0.0.0/8`, `[::1]` and `[::]` should be denied by default unless `--allow-loopback-peers` has been specified.	7.2	More Details
CVE-2021-1160	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1170	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1161	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1162	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1163	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1169	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1168	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1167	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1166	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1164	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1147	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1148	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1173	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1183	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1193	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1192	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1191	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1190	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1188	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1187	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1186	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1185	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1174	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1184	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1182	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1181	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1180	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1179	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1178	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1177	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1176	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2021-1175	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1165	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.	7.2	More Details
CVE-2020-25533	An issue was discovered in Malwarebytes before 4.0 on macOS. A malicious application was able to perform a privileged action within the Malwarebytes launch daemon. The privileged service improperly validated XPC connections by relying on the PID instead of the audit token. An attacker can construct a situation where the same PID is used for running two different programs at different times, by leveraging a race condition during crafted use of posix_spawn.	7.0	More Details
CVE-2021-21011	Adobe Captivate 2019 version 11.5.1.499 (and earlier) is affected by an uncontrolled search path element vulnerability that could lead to privilege escalation. An attacker with permissions to write to the file system could leverage this vulnerability to escalate privileges.	7.0	More Details
CVE-2021-21010	InCopy version 15.1.1 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.0	More Details
CVE-2021-21008	Adobe Animate version 21.0 (and earlier) is affected by an uncontrolled search path element that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.0	More Details
CVE-2021-21007	Adobe Illustrator version 25.0 (and earlier) is affected by an uncontrolled search path element that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.0	More Details
CVE-2020-27256	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, a hard-coded physician PIN in the physician menu of the insulin pump allows attackers with physical access to change insulin therapy settings.	6.8	More Details
CVE-2021-0220	The Junos Space Network Management Platform has been found to store shared secrets in a recoverable format that can be exposed through the UI. An attacker who is able to execute arbitrary code in the victim browser (for example via XSS) or access cached contents may be able to obtain a copy of credentials managed by Junos Space. The impact of a successful attack includes, but is not limited to, obtaining access to other servers connected to the Junos Space Management Platform. This issue affects Juniper Networks Junos Space versions prior to 20.3R1.	6.8	More Details
CVE-2020-28473	The package bottle from 0 and before 0.12.19 are vulnerable to Web Cache Poisoning by using a vector called parameter cloaking. When the attacker can separate query parameters using a semicolon (;), they can cause a difference in the interpretation of the request between the proxy (running with default configuration) and the server. This can result in malicious requests being cached as completely safe ones, as the proxy would usually not see the semicolon as a separator, and therefore would not include it in a cache key of an unkeyed parameter.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0210	An Information Exposure vulnerability in J-Web of Juniper Networks Junos OS allows an unauthenticated attacker to elevate their privileges over the target system through opportunistic use of an authenticated users session. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S17; 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R2-S4, 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R1-S5, 19.2R3, 19.2R3-S1; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2.	6.8	More Details
CVE-2020-15218	Combodo iTop is a web based IT Service Management tool. In iTop before versions 2.7.2 and 3.0.0, admin pages are cached, so that their content is visible after deconnection by using the browser back button. This is fixed in versions 2.7.2 and 3.0.0.	6.8	More Details
CVE-2020-15221	Combodo iTop is a web based IT Service Management tool. In iTop before versions 2.7.2 and 3.0.0, by modifying target browser local storage, an XSS can be generated in the iTop console breadcrumb. This is fixed in versions 2.7.2 and 3.0.0.	6.8	More Details
CVE-2020-23522	Pixelimity 1.0 has cross-site request forgery via the admin/setting.php data [Password] parameter.	6.8	More Details
CVE-2020-9209	There is a privilege escalation vulnerability in SMC2.0 product. Some files in a directory of a module are located improperly. It does not apply the directory limitation. Attackers can exploit this vulnerability by crafting malicious file to launch privilege escalation. This can compromise normal service of affected products.	6.7	More Details
CVE-2021-0219	A command injection vulnerability in install package validation subsystem of Juniper Networks Junos OS that may allow a locally authenticated attacker with privileges to execute commands with root privilege. To validate a package in Junos before installation, an administrator executes the command 'request system software add validate-on-host' via the CLI. An attacker with access to this CLI command may be able to exploit this vulnerability. This issue affects Juniper Networks Junos OS: all versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S8, 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R2-S2, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2.	6.7	More Details
CVE-2021-0209	In Juniper Networks Junos OS Evolved an attacker sending certain valid BGP update packets may cause Junos OS Evolved to access an uninitialized pointer causing RPD to core leading to a Denial of Service (DoS). Continued receipt of these types of valid BGP update packets will cause an extended Denial of Service condition. RPD will require a restart to recover. An indicator of compromise is to see if the file rpd.re exists by issuing the command: show system core-dumps This issue affects: Juniper Networks Junos OS Evolved 19.4 versions prior to 19.4R2-S2-EVO; 20.1 versions prior to 20.1R1-S2-EVO, 20.1R2-S1-EVO. This issue does not affect Junos OS.	6.5	More Details
CVE-2020-27258	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, an information disclosure vulnerability in the communication protocol of the insulin pump and its AnyDana-i and AnyDana-A mobile applications allows unauthenticated attackers to extract the pump’s keypad lock PIN via Bluetooth Low Energy.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23837	An issue was discovered in flatCore before 2.0.0 build 139. A time-based blind SQL injection was identified in the selected_folder HTTP request body parameter for the acp interface. The affected parameter (which retrieves the file contents of the specified folder) was found to be accepting malicious user input without proper sanitization, thus leading to SQL injection. Database related information can be successfully retrieved.	6.5	More Details
CVE-2020-1865	There is an out-of-bounds read vulnerability in Huawei CloudEngine products. The software reads data past the end of the intended buffer when parsing certain PIM message, an adjacent attacker could send crafted PIM messages to the device, successful exploit could cause out of bounds read when the system does the certain operation.	6.5	More Details
CVE-2021-0221	In an EVPN/VXLAN scenario, if an IRB interface with a virtual gateway address (VGA) is configured on a PE, a traffic loop may occur upon receipt of specific IP multicast traffic. The traffic loop will cause interface traffic to increase abnormally, ultimately leading to a Denial of Service (DoS) in packet processing. The following command could be used to monitor the interface traffic: user@junos> monitor interface traffic Interface Link Input packets (pps) Output packets (pps) et-0/0/1 Up 6492089274364 (70994959) 6492089235319 (70994956) et-0/0/25 Up 343458103 (1) 156844 (0) ae0 Up 9132519197257 (70994959) 9132519139454 (70994956) This issue affects Juniper Networks Junos OS on QFX Series: all versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R1-S5, 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2.	6.5	More Details
CVE-2020-27266	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, a client-side control vulnerability in the insulin pump and its AnyDana-i and AnyDana-A mobile applications allows physically proximate attackers to bypass user authentication checks via Bluetooth Low Energy.	6.5	More Details
CVE-2021-21602	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows reading arbitrary files using the file browser for workspaces and archived artifacts by following symlinks.	6.5	More Details
CVE-2021-1245	Cisco Finesse and Cisco Unified CVP OpenSocial Gadget Editor Cross-Site Scripting Vulnerability A vulnerability in the web-based management interface of Cisco Finesse and Cisco Unified CVP could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.5	More Details
CVE-2020-1866	There is an out-of-bounds read vulnerability in several products. The software reads data past the end of the intended buffer when parsing certain crafted DHCP messages. Successful exploit could cause certain service abnormal. Affected product versions include:NIP6800 versions V500R001C30,V500R001C60SPC500,V500R005C00;S12700 versions V200R008C00;S2700 versions V200R008C00;S5700 versions V200R008C00;S6700 versions V200R008C00;S7700 versions V200R008C00;S9700 versions V200R008C00;Secospace USG6600 versions V500R001C30SPC200,V500R001C30SPC600,V500R001C60SPC500,V500R005C00;USG9500 versions V500R001C30SPC300,V500R001C30SPC600,V500R001C60SPC500,V500R005C00.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0215	On Juniper Networks Junos EX series, QFX Series, MX Series and SRX branch series devices, a memory leak occurs every time the 802.1X authenticator port interface flaps which can lead to other processes, such as the pfex process, responsible for packet forwarding, to crash and restart. An administrator can use the following CLI command to monitor the status of memory consumption: user@device> show task memory detail Please refer to https://kb.juniper.net/KB31522 for details. This issue affects Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D54; 15.1X49 versions prior to 15.1X49-D240 ; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10 ; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S2; 19.1 versions prior to 19.1R1-S5, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2. This issue does not affect Juniper Networks Junos OS 12.3, 15.1.	6.5	More Details
CVE-2021-1145	A vulnerability in the Secure FTP (SFTP) of Cisco StarOS for Cisco ASR 5000 Series Routers could allow an authenticated, remote attacker to read arbitrary files on an affected device. To exploit this vulnerability, the attacker would need to have valid credentials on the affected device. The vulnerability is due to insecure handling of symbolic links. An attacker could exploit this vulnerability by sending a crafted SFTP command to an affected device. A successful exploit could allow the attacker to read arbitrary files on the affected device.	6.5	More Details
CVE-2021-3181	rfc822.c in Mutt through 2.0.4 allows remote attackers to cause a denial of service (mailbox unavailability) by sending email messages with sequences of semicolon characters in RFC822 address fields (aka terminators of empty groups). A small email message from the attacker can cause large memory consumption, and the victim may then be unable to see email messages from other persons.	6.5	More Details
CVE-2020-27268	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, a client-side control vulnerability in the insulin pump and its AnyDana-i and AnyDana-A mobile applications allows physically proximate attackers to bypass checks for default PINs via Bluetooth Low Energy.	6.5	More Details
CVE-2021-21607	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not limit sizes provided as query parameters to graph-rendering URLs, allowing attackers to request crafted URLs that use all available memory in Jenkins, potentially leading to out of memory errors.	6.5	More Details
CVE-2021-1131	A vulnerability in the Cisco Discovery Protocol implementation for Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause an affected IP camera to reload. The vulnerability is due to missing checks when Cisco Discovery Protocol messages are processed. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected IP camera. A successful exploit could allow the attacker to cause the affected IP camera to reload unexpectedly, resulting in a denial of service (DoS) condition. Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	6.5	More Details
CVE-2020-8581	Clustered Data ONTAP versions prior to 9.3P20 and 9.5 are susceptible to a vulnerability which could allow an authenticated but unauthorized attacker to overwrite arbitrary data when VMware vStorage support is enabled.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1246	Cisco Finesse, Cisco Virtualized Voice Browser, and Cisco Unified CVP OpenSocial Gadget Editor Unauthenticated Access Vulnerability A vulnerability in the web management interface of Cisco Finesse, Cisco Virtualized Voice Browser, and Cisco Unified CVP could allow an unauthenticated, remote attacker to access the OpenSocial Gadget Editor without providing valid user credentials. The vulnerability is due to missing authentication for a specific section of the web-based management interface. An attacker could exploit this vulnerability by accessing a crafted URL. A successful exploit could allow the attacker to obtain access to a section of the interface, which they could use to obtain potentially confidential information and create arbitrary XML files. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.5	More Details
CVE-2020-29450	Affected versions of Atlassian Confluence Server and Data Center allow remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability in the avatar upload feature. The affected versions are before version 7.2.0.	6.5	More Details
CVE-2021-3178	fs/nfsd/nfs3xdr.c in the Linux kernel through 5.10.8, when there is an NFS export of a subdirectory of a filesystem, allows remote attackers to traverse to other parts of the filesystem via READDIRPLUS. NOTE: some parties argue that such a subdirectory export is not intended to prevent this attack; see also the exports(5) no_subtree_check default behavior	6.5	More Details
CVE-2020-16119	Use-after-free vulnerability in the Linux kernel exploitable by a local attacker due to reuse of a DCCP socket with an attached dccps_hc_tx_ccid object as a listener after being released. Fixed in Ubuntu Linux kernel 5.4.0-51.56, 5.3.0-68.63, 4.15.0-121.123, 4.4.0-193.224, 3.13.0.182.191 and 3.2.0-149.196.	6.3	More Details
CVE-2020-28707	The Stockdio Historical Chart plugin before 2.8.1 for WordPress is affected by Cross Site Scripting (XSS) via stockdio_chart_historical-wp.js in wp-content/plugins/stockdio-historical-chart/assets/ because the origin of a postMessage() event is not validated. The stockdio_eventer function listens for any postMessage event. After a message event is sent to the application, this function sets the "e" variable as the event and checks that the types of the data and data.method are not undefined (empty) before proceeding to eval the data.method received from the postMessage. However, on a different website. JavaScript code can call window.open for the vulnerable WordPress instance and do a postMessage(msg,'*') for that object.	6.1	More Details
CVE-2021-21610	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not implement any restrictions for the URL rendering a formatted preview of markup passed as a query parameter, resulting in a reflected cross-site scripting (XSS) vulnerability if the configured markup formatter does not prohibit unsafe elements (JavaScript) in markup.	6.1	More Details
CVE-2021-20619	Cross-site scripting vulnerability in GROWI (v4.2 Series) versions prior to v4.2.3 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2020-16255	ownCloud (Core) before 10.5 allows XSS in login page 'forgot password.'	6.1	More Details
CVE-2021-25324	MISP 2.4.136 has Stored XSS in the galaxy cluster view via a cluster name to app/View/GalaxyClusters/view.ctp.	6.1	More Details
CVE-2020-27219	In all version of Eclipse Hawkbit prior to 0.3.0M7, the HTTP 404 (Not Found) JSON response body returned by the REST API may contain unsafe characters within the path attribute. Sending a POST request to a non existing resource will return the full path from the given URL unescaped to the client.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25325	MISP 2.4.136 has XSS via galaxy cluster element values to app/View/GalaxyElements/ajax/index.ctp. Reference types could contain javascript: URLs.	6.1	More Details
CVE-2020-16046	Script injection in iOSWeb in Google Chrome on iOS prior to 84.0.4147.105 allowed a remote attacker to execute arbitrary code via a crafted HTML page.	6.1	More Details
CVE-2021-3184	MISP 2.4.136 has XSS via a crafted URL to the app/View/Elements/global_menu.ctp user homepage favourite button.	6.1	More Details
CVE-2021-21613	Jenkins TICS Plugin 2020.3.0.6 and earlier does not escape TICS service responses, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers able to control TICS service response content.	6.1	More Details
CVE-2020-15864	An issue was discovered in Quali CloudShell 9.3. An XSS vulnerability in the login page allows an attacker to craft a URL, with a constructor.constructor substring in the username field, that executes a payload when the user visits the /Account/Login page.	6.1	More Details
CVE-2021-25295	OpenCATS through 0.9.5-3 has multiple Cross-site Scripting (XSS) issues.	6.1	More Details
CVE-2020-15220	Combodo iTop is a web based IT Service Management tool. In iTop before versions 2.7.2 and 3.0.0, two cookies are created for the same session, which leads to a possibility to steal user session. This is fixed in versions 2.7.2 and 3.0.0.	6.1	More Details
CVE-2020-28482	This affects the package fastify-csrf before 3.0.0. 1. The generated cookie used insecure defaults, and did not have the httpOnly flag on: cookieOpts: { path: '/', sameSite: true } 2. The CSRF token was available in the GET query parameter	5.9	More Details
CVE-2020-28479	The package jointjs before 3.3.0 are vulnerable to Denial of Service (DoS) via the unsetByPath function.	5.9	More Details
CVE-2021-24122	When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.	5.9	More Details
CVE-2020-20950	Bleichenbacher's attack on PKCS #1 v1.5 padding for RSA in Microchip Libraries for Applications 2018-11-26 All up to 2018-11-26. The vulnerability can allow one to use Bleichenbacher's oracle attack to decrypt an encrypted ciphertext by making successive queries to the server using the vulnerable library, resulting in remote information disclosure.	5.9	More Details
CVE-2021-1224	Multiple Cisco products are affected by a vulnerability with TCP Fast Open (TFO) when used in conjunction with the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect detection of the HTTP payload if it is contained at least partially within the TFO connection handshake. An attacker could exploit this vulnerability by sending crafted TFO packets with an HTTP payload through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0205	When the "Intrusion Detection Service" (IDS) feature is configured on Juniper Networks MX series with a dynamic firewall filter using IPv6 source or destination prefix, it may incorrectly match the prefix as /32, causing the filter to block unexpected traffic. This issue affects only IPv6 prefixes when used as source and destination. This issue affects MX Series devices using MS-MPC, MS-MIC or MS-SPC3 service cards with IDS service configured. This issue affects: Juniper Networks Junos OS 17.3 versions prior to 17.3R3-S10 on MX Series; 17.4 versions prior to 17.4R3-S3 on MX Series; 18.1 versions prior to 18.1R3-S11 on MX Series; 18.2 versions prior to 18.2R3-S6 on MX Series; 18.3 versions prior to 18.3R3-S4 on MX Series; 18.4 versions prior to 18.4R3-S6 on MX Series; 19.1 versions prior to 19.1R2-S2, 19.1R3-S3 on MX Series; 19.2 versions prior to 19.2R3-S1 on MX Series; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1 on MX Series; 19.4 versions prior to 19.4R3 on MX Series; 20.1 versions prior to 20.1R2 on MX Series; 20.2 versions prior to 20.2R2 on MX Series;	5.8	More Details
CVE-2020-27270	SOOIL Developments CoLtd DiabecareRS, AnyDana-i ,AnyDana-A, communication protocol of the insulin pump & AnyDana-i,AnyDana-A mobile apps doesnt use adequate measures to protect encryption keys in transit which allows unauthenticated physically proximate attacker to sniff keys via (BLE).	5.7	More Details
CVE-2020-27272	SOOIL Developments CoLtd DiabecareRS, AnyDana-i, AnyDana-A, The communication protocol of the insulin pump and AnyDana-i,AnyDana-A mobile apps doesn't use adequate measures to authenticate the pump before exchanging keys, which allows unauthenticated, physically proximate attackers to eavesdrop the keys and spoof the pump via BLE.	5.7	More Details
CVE-2020-27269	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, the communication protocol of the insulin pump and its AnyDana-i and AnyDana-A mobile applications lacks replay protection measures, which allows unauthenticated, physically proximate attackers to replay communication sequences via Bluetooth Low Energy.	5.7	More Details
CVE-2020-27276	SOOIL Developments Co Ltd DiabecareRS,AnyDana-i & AnyDana-A, the communication protocol of the insulin pump and its AnyDana-i & AnyDana-A mobile apps doesn't use adequate measures to authenticate the communicating entities before exchanging keys, which allows unauthenticated, physically proximate attackers to eavesdrop the authentication sequence via Bluetooth Low Energy.	5.7	More Details
CVE-2020-27368	Directory Indexing in Login Portal of Login Portal of TOTOLINK-A702R-V1.0.0-B20161227.1023 allows attacker to access /icons/ directories via GET Parameter.	5.5	More Details
CVE-2021-21614	Jenkins Bumblebee HP ALM Plugin 4.1.5 and earlier stores credentials unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	5.5	More Details
CVE-2021-1126	A vulnerability in the storage of proxy server credentials of Cisco Firepower Management Center (FMC) could allow an authenticated, local attacker to view credentials for a configured proxy server. The vulnerability is due to clear-text storage and weak permissions of related configuration files. An attacker could exploit this vulnerability by accessing the CLI of the affected software and viewing the contents of the affected files. A successful exploit could allow the attacker to view the credentials that are used to access the proxy server.	5.5	More Details
CVE-2013-1053	In crypt.c of remote-login-service, the cryptographic algorithm used to cache usernames and passwords is insecure. An attacker could use this vulnerability to recover usernames and passwords from the file. This issue affects version 1.0.0-0ubuntu3 and prior versions.	5.5	More Details
CVE-2020-4871	IBM Planning Analytics 2.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 190834.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7343	Missing Authorization vulnerability in McAfee Agent (MA) for Windows prior to 5.7.1 allows local users to block McAfee product updates by manipulating a directory used by MA for temporary files. The product would continue to function with out-of-date detection files.	5.5	More Details
CVE-2021-1258	A vulnerability in the upgrade component of Cisco AnyConnect Secure Mobility Client could allow an authenticated, local attacker with low privileges to read arbitrary files on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient file permission restrictions. An attacker could exploit this vulnerability by sending a crafted command from the local CLI to the application. A successful exploit could allow the attacker to read arbitrary files on the underlying OS of the affected device. The attacker would need to have valid user credentials to exploit this vulnerability.	5.5	More Details
CVE-2021-21612	Jenkins TraceTronic ECU-TEST Plugin 2.23.1 and earlier stores credentials unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	5.5	More Details
CVE-2021-21603	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape notification bar response contents, resulting in a cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2021-21608	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape button labels in the Jenkins UI, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers with the ability to control button labels.	5.4	More Details
CVE-2020-14410	SDL (Simple DirectMedia Layer) through 2.0.12 has a heap-based buffer over-read in Blit_3or4_to_3or4__inversed_rgb in video/SDL_blit_N.c via a crafted .BMP file.	5.4	More Details
CVE-2020-26733	Cross Site Scripting (XSS) in Configuration page in SKYWORTH GN542VF Hardware Version 2.0 and Software Version 2.0.0.16 allows authenticated attacker to inject their own script into the page via DDNS Configuration Section.	5.4	More Details
CVE-2021-1311	A vulnerability in the reclaim host role feature of Cisco Webex Meetings and Cisco Webex Meetings Server could allow an authenticated, remote attacker to take over the host role during a meeting. This vulnerability is due to a lack of protection against brute forcing of the host key. An attacker could exploit this vulnerability by sending crafted requests to a vulnerable Cisco Webex Meetings or Webex Meetings Server site. A successful exploit would require the attacker to have access to join a Webex meeting, including applicable meeting join links and passwords. A successful exploit could allow the attacker to acquire or take over the host role for a meeting.	5.4	More Details
CVE-2020-29587	SimplCommerce 1.0.0-rc uses the Bootbox.js library, which allows creation of programmatic dialog boxes using Bootstrap modals. The Bootbox.js library intentionally does not perform any sanitization of user input, which results in a DOM XSS, because it uses the jQuery .html() function to directly append the payload to a dialog.	5.4	More Details
CVE-2020-35748	Cross-site scripting (XSS) vulnerability in models/list-table.php in the FV Flowplayer Video Player plugin before 7.4.37.727 for WordPress allows remote authenticated users to inject arbitrary web script or HTML via the fv_wp_fvvideoplayer_src JSON field in the data parameter.	5.4	More Details
CVE-2020-35582	A stored cross-site scripting (XSS) issue in Envira Gallery Lite before 1.8.3.3 allows remote attackers to inject arbitrary JavaScript/HTML code via a POST /wp-admin/post.php request with the post_title parameter.	5.4	More Details
CVE-2021-21611	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape display names and IDs of item types shown on the New Item page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to specify display names or IDs of item types.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-16961	SolarWinds Web Help Desk 12.7.0 allows XSS via a Schedule Name.	5.4	More Details
CVE-2021-1127	A vulnerability in the web-based management interface of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. The vulnerability is due to improper input validation of log file content stored on the affected device. An attacker could exploit this vulnerability by modifying a log file with malicious code and getting a user to view the modified log file. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or to access sensitive, browser-based information.	5.4	More Details
CVE-2020-35581	A stored cross-site scripting (XSS) issue in Envira Gallery Lite before 1.8.3.3 allows remote attackers to inject arbitrary JavaScript/HTML code via a POST /wp-admin/admin-ajax.php request with the meta[title] parameter.	5.4	More Details
CVE-2021-21252	The jQuery Validation Plugin provides drop-in validation for your existing forms. It is published as an npm package "jquery-validation". jquery-validation before version 1.19.3 contains one or more regular expressions that are vulnerable to ReDoS (Regular Expression Denial of Service). This is fixed in 1.19.3.	5.3	More Details
CVE-2019-4687	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 171823.	5.3	More Details
CVE-2021-1236	Multiple Cisco products are affected by a vulnerability in the Snort application detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. The vulnerability is due to a flaw in the detection algorithm. An attacker could exploit this vulnerability by sending crafted packets that would flow through an affected system. A successful exploit could allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network.	5.3	More Details
CVE-2021-22167	An issue has been discovered in GitLab affecting all versions starting from 12.1. Incorrect headers in specific project page allows attacker to have a temporary read access to the private repository	5.3	More Details
CVE-2021-22166	An attacker could cause a Prometheus denial of service in GitLab 13.7+ by sending an HTTP request with a malformed method	5.3	More Details
CVE-2020-36192	An issue was discovered in the Source Integration plugin before 2.4.1 for MantisBT. An attacker can gain access to the Summary field of private Issues (either marked as Private, or part of a private Project), if they are attached to an existing Changeset. The information is visible on the view.php page, as well as on the list.php page (a pop-up on the Affected Issues id hyperlink). Additionally, if the attacker has "Update threshold" in the plugin's configuration (set to the "updater" access level by default), then they can link any Issue to a Changeset by entering the Issue's Id, even if they do not have access to it.	5.3	More Details
CVE-2020-4873	IBM Planning Analytics 2.0 could allow an attacker to obtain sensitive information due to an overly permissive CORS policy. IBM X-Force ID: 190836.	5.3	More Details
CVE-2021-22850	HGiga EIP product lacks ineffective access control in certain pages that allow attackers to access database or perform privileged functions.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21609	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not correctly match requested URLs to the list of always accessible paths, allowing attackers without Overall/Read permission to access some URLs as if they did have Overall/Read permission.	5.3	More Details
CVE-2020-28481	The package socket.io before 2.4.0 are vulnerable to Insecure Defaults due to CORS Misconfiguration. All domains are whitelisted by default.	5.3	More Details
CVE-2020-4599	IBM Security Guardium Insights 2.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 184824.	5.3	More Details
CVE-2020-29019	A stack-based buffer overflow vulnerability in FortiWeb 6.3.0 through 6.3.7 and version before 6.2.4 may allow a remote, unauthenticated attacker to crash the httpd daemon thread by sending a request with a crafted cookie header.	5.3	More Details
CVE-2020-4600	IBM Security Guardium Insights 2.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 184832.	5.3	More Details
CVE-2020-29446	Affected versions of Atlassian Fisheye & Crucible allow remote attackers to browse local files via an Insecure Direct Object References (IDOR) vulnerability in the WEB-INF directory. The affected versions are before version 4.8.5.	5.3	More Details
CVE-2020-9143	There is a missing authentication vulnerability in some Huawei smartphone.Successful exploitation of this vulnerability may lead to low-sensitive information exposure.	5.3	More Details
CVE-2020-9138	There is a heap-based buffer overflow vulnerability in some Huawei Smartphone, Successful exploit of this vulnerability can cause process exceptions during updating.	5.3	More Details
CVE-2021-0212	An Information Exposure vulnerability in Juniper Networks Contrail Networking allows a locally authenticated attacker able to read files to retrieve administrator credentials stored in plaintext thereby elevating their privileges over the system. This issue affects: Juniper Networks Contrail Networking versions prior to 1911.31.	5.0	More Details
CVE-2021-23835	An issue was discovered in flatCore before 2.0.0 build 139. A local file disclosure vulnerability was identified in the docs_file HTTP request body parameter for the acp interface. This can be exploited with admin access rights. The affected parameter (which retrieves the contents of the specified file) was found to be accepting malicious user input without proper sanitization, thus leading to retrieval of backend server sensitive files, e.g., /etc/passwd, SQLite database files, PHP source code, etc.	4.9	More Details
CVE-2021-1151	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1155	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	4.8	More Details
CVE-2021-1152	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	4.8	More Details
CVE-2021-1157	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	4.8	More Details
CVE-2020-6777	A vulnerability in the web-based management interface of Bosch PRAESIDEO until and including version 4.41 and Bosch PRAESENSA until and including version 1.10 allows an authenticated remote attacker with admin privileges to mount a stored Cross-Site-Scripting (XSS) attack against another user. When the victim logs into the management interface, the stored script code is executed in the context of his browser. A successful exploit would allow an attacker to interact with the management interface with the privileges of the victim. However, as the attacker already needs admin privileges, there is no additional impact on the management interface itself.	4.8	More Details
CVE-2021-1156	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	4.8	More Details
CVE-2021-22132	Elasticsearch versions 7.7.0 to 7.10.1 contain an information disclosure flaw in the async search API. Users who execute an async search will improperly store the HTTP headers. An Elasticsearch user with the ability to read the .tasks index could obtain sensitive request headers of other users in the cluster. This issue is fixed in Elasticsearch 7.10.2	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1154	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	4.8	More Details
CVE-2021-1153	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	4.8	More Details
CVE-2021-23836	An issue was discovered in flatCore before 2.0.0 build 139. A stored XSS vulnerability was identified in the prefs_smtp_psw HTTP request body parameter for the acp interface. An admin user can inject malicious client-side script into the affected parameter without any form of input sanitization. The injected payload will be executed in the browser of a user whenever one visits the affected module page.	4.8	More Details
CVE-2021-23838	An issue was discovered in flatCore before 2.0.0 build 139. A reflected XSS vulnerability was identified in the media_filter HTTP request body parameter for the acp interface. The affected parameter accepts malicious client-side script without proper input sanitization. For example, a malicious user can leverage this vulnerability to steal cookies from a victim user and perform a session-hijacking attack, which may then lead to unauthorized access to the site.	4.8	More Details
CVE-2021-1158	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	4.8	More Details
CVE-2021-1130	A vulnerability in the web-based management interface of Cisco DNA Center software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker would need to have administrative credentials on the affected device.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1240	A vulnerability in the loading process of specific DLLs in Cisco Proximity Desktop for Windows could allow an authenticated, local attacker to load a malicious library. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file in a specific location on the targeted system. This file will execute when the vulnerable application launches. A successful exploit could allow the attacker to execute arbitrary code on the targeted system with the privileges of another user’s account.	4.8	More Details
CVE-2021-1239	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected system. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	4.8	More Details
CVE-2021-1238	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected system. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	4.8	More Details
CVE-2021-1310	A vulnerability in the web-based management interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to redirect a user to an untrusted web page, bypassing the warning mechanism that should prompt the user before the redirection. This vulnerability is due to improper input validation of the URL parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website, bypassing the Webex URL check that should result in a warning before the redirection to the web page. Attackers may use this type of vulnerability, known as an open redirect attack, as part of a phishing attack to convince users to unknowingly visit malicious sites.	4.7	More Details
CVE-2020-36191	JupyterHub 1.1.0 allows CSRF in the admin panel via a request that lacks an _xsrf field, as demonstrated by a /hub/api/user request (to add or remove a user account).	4.5	More Details
CVE-2020-4604	IBM Security Guardium Insights 2.0.2 stores user credentials in plain in clear text which can be read by a local privileged user. IBM X-Force ID: 184861.	4.4	More Details
CVE-2020-4602	IBM Security Guardium Insights 2.0.2 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 184836.	4.4	More Details
CVE-2021-3032	An information exposure through log file vulnerability exists in Palo Alto Networks PAN-OS software where configuration secrets for the “http”, “email”, and “snmptrap” v3 log forwarding server profiles can be logged to the logrcvr.log system log. Logged information may include up to 1024 bytes of the configuration including the username and password in an encrypted form and private keys used in any certificate profiles set for log forwarding server profiles. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.4; PAN-OS 10.0 versions earlier than PAN-OS 10.0.1.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21722	A ZTE Smart STB is impacted by an information leak vulnerability. The device did not fully verify the log, so attackers could use this vulnerability to obtain sensitive user information for further information detection and attacks. This affects: ZXV10 B860A V2.1-T_V0032.1.1.04_jiangsuTelecom.	4.4	More Details
CVE-2021-1242	A vulnerability in Cisco Webex Teams could allow an unauthenticated, remote attacker to manipulate file names within the messaging interface. The vulnerability exists because the affected software mishandles character rendering. An attacker could exploit this vulnerability by sharing a file within the application interface. A successful exploit could allow the attacker to modify how the shared file name displays within the interface, which could allow the attacker to conduct phishing or spoofing attacks.	4.3	More Details
CVE-2021-1267	A vulnerability in the dashboard widget of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper restrictions on XML entities. An attacker could exploit this vulnerability by crafting an XML-based widget on an affected server. A successful exploit could cause increased memory and CPU utilization, which could result in a DoS condition.	4.3	More Details
CVE-2021-21606	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier improperly validates the format of a provided fingerprint ID when checking for its existence allowing an attacker to check for the existence of XML files with a short path.	4.3	More Details
CVE-2020-11997	Apache Guacamole 1.2.0 and earlier do not consistently restrict access to connection history based on user visibility. If multiple users share access to the same connection, those users may be able to see which other users have accessed that connection, as well as the IP addresses from which that connection was accessed, even if those users do not otherwise have permission to see other users.	4.3	More Details
CVE-2021-1226	A vulnerability in the audit logging component of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, Cisco Emergency Responder, and Cisco Prime License Manager could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. The vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs on an affected system and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices.	4.3	More Details
CVE-2020-35687	PHPFusion version 9.03.90 is vulnerable to CSRF attack which leads to deletion of all shoutbox messages by the attacker on behalf of the logged in victim.	4.3	More Details
CVE-2020-15219	Combodo iTop is a web based IT Service Management tool. In iTop before versions 2.7.2 and 3.0.0, when a download error is triggered in the user portal, an SQL query is displayed to the user. This is fixed in versions 2.7.2 and 3.0.0.	4.3	More Details
CVE-2020-26414	An issue has been discovered in GitLab affecting all versions starting from 12.4. The regex used for package names is written in a way that makes execution time have quadratic growth based on the length of the malicious input string.	4.3	More Details
CVE-2021-22168	A regular expression denial of service issue has been discovered in NuGet API affecting all versions of GitLab starting from version 12.8.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1143	A vulnerability in Cisco Connected Mobile Experiences (CMX) API authorizations could allow an authenticated, remote attacker to enumerate what users exist on the system. The vulnerability is due to a lack of authorization checks for certain API GET requests. An attacker could exploit this vulnerability by sending specific API GET requests to an affected device. A successful exploit could allow the attacker to enumerate users of the CMX system.	4.3	More Details
CVE-2020-4597	IBM Security Guardium Insights 2.0.2 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 184822.	4.3	More Details
CVE-2021-3031	Padding bytes in Ethernet packets on PA-200, PA-220, PA-500, PA-800, PA-2000 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls are not cleared before the data frame is created. This leaks a small amount of random information from the firewall memory into the Ethernet packets. An attacker on the same Ethernet subnet as the PAN-OS firewall is able to collect potentially sensitive information from these packets. This issue is also known as Etherleak and is detected by security scanners as CVE-2003-0001. This issue impacts: PAN-OS 8.1 version earlier than PAN-OS 8.1.18; PAN-OS 9.0 versions earlier than PAN-OS 9.0.12; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5.	4.3	More Details
CVE-2020-9203	There is a resource management errors vulnerability in Huawei P30. Local attackers construct broadcast message for some application, causing this application to send this broadcast message and impact the customer's use experience.	3.3	More Details
CVE-2021-21012	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to an insecure direct object vulnerability (IDOR) in the checkout module. Successful exploitation could lead to sensitive information disclosure.	N/A	More Details
CVE-2021-20189	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-28476	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-23336. Reason: This candidate is a reservation duplicate of CVE-2021-23336. Notes: All CVE users should reference CVE-2021-23336 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-29598	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its requester. Notes: none	N/A	More Details