SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 October 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-2021-42369	Imagicle Application Suite (for Cisco UC) before 2021.Summer.2 allows SQL injection. A low-privileged user could inject a SQL statement through the "Export to CSV" feature of the Contact Manager web GUI.	9.9	More Details
CVE-2021-40996	A remote authentication bypass vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	9.8	More Details
CVE-2021-40720	Ops CLI version 2.0.4 (and earlier) is affected by a Deserialization of Untrusted Data vulnerability to achieve arbitrary code execution when the checkout_repo function is called on a maliciously crafted file. An attacker can leverage this to execute arbitrary code on the victim machine.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30820	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.8 and iPadOS 14.8. A remote attacker may be able to cause arbitrary code execution.	9.8	More Details
CVE-2021-38462	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 does not enforce an efficient password policy. This may allow an attacker with obtained user credentials to enumerate passwords and impersonate other application users and perform operations on their behalf.	9.8	More Details
CVE-2021-23449	This affects the package vm2 before 3.9.4 via a Prototype Pollution attack vector, which can lead to execution of arbitrary code on the host machine.	9.8	More Details
CVE-2021-42576	The bluemonday sanitizer before 1.0.16 for Go, and before 0.0.8 for Python (in pybluemonday), does not properly enforce policies associated with the SELECT, STYLE, and OPTION elements.	9.8	More Details
CVE-2021-42575	The OWASP Java HTML Sanitizer before 20211018.1 does not properly enforce policies associated with the SELECT, STYLE, and OPTION elements.	9.8	More Details
CVE-2021-38389	Advantech WebAccess versions 9.02 and prior are vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute code.	9.8	More Details
CVE-2021-33023	Advantech WebAccess versions 9.02 and prior are vulnerable to a heap-based buffer overflow, which may allow an attacker to remotely execute code.	9.8	More Details
CVE-2021-22961	A code injection vulnerability exists within the firewall software of GlassWire v2.1.167 that could lead to arbitrary code execution from a file in the user path on first execution.	9.8	More Details
CVE-2021-38297	Go before 1.16.9 and 1.17.x before 1.17.2 has a Buffer Overflow via large arguments in a function invocation from a WASM module, when GOARCH=wasm GOOS=js is used.	9.8	More Details
CVE-2021-27561	Yealink Device Management (DM) 3.6.0.20 allows command injection as root via the /sm/api/v1/firewall/zone/services URI, without authentication.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40997	A remote authentication bypass vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	9.8	More Details
CVE-2021-20125	An arbitrary file upload and directory traversal vulnerability exists in the file upload functionality of DownloadFileServlet in Draytek VigorConnect 1.6.0-B3. An unauthenticated attacker could leverage this vulnerability to upload files to any location on the target operating system with root privileges.	9.8	More Details
CVE-2021-31349	The usage of an internal HTTP header created an authentication bypass vulnerability (CWE-287), allowing an attacker to view internal files, change settings, manipulate services and execute arbitrary code. This issue affects all Juniper Networks 128 Technology Session Smart Router versions prior to 4.5.11, and all versions of 5.0 up to and including 5.0.1.	9.8	More Details
CVE-2021-38432	FATEK Automation Communication Server Versions 1.13 and prior lacks proper validation of user-supplied data, which could result in a stack-based buffer overflow condition and allow an attacker to remotely execute code.	9.8	More Details
CVE-2021-42342	An issue was discovered in GoAhead 4.x and 5.x before 5.1.5. In the file upload filter, user form variables can be passed to CGI scripts without being prefixed with the CGI prefix. This permits tunneling untrusted environment variables into vulnerable CGI scripts.	9.8	More Details
CVE-2021-35498	The TIBCO EBX Web Server component of TIBCO Software Inc.'s TIBCO EBX, TIBCO EBX, TIBCO EBX, and TIBCO Product and Service Catalog powered by TIBCO EBX contains a vulnerability that under certain specific conditions allows an attacker to enter a password other than the legitimate password and it will be accepted as valid. Affected releases are TIBCO Software Inc.'s TIBCO EBX: versions 5.8.123 and below, TIBCO EBX: versions 5.9.3, 5.9.4, 5.9.5, 5.9.6, 5.9.7, 5.9.8, 5.9.9, 5.9.10, 5.9.11, 5.9.12, 5.9.13, and 5.9.14, TIBCO EBX: versions 6.0.0 and 6.0.1, and TIBCO Product and Service Catalog powered by TIBCO EBX: version 1.0.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40842	Proofpoint Insider Threat Management Server contains a SQL injection vulnerability in the Web Console. The vulnerability exists due to improper input validation on the database name parameter required in certain unauthenticated APIs. A malicious URL visited by anyone with network access to the server could be used to blindly execute arbitrary SQL statements on the backend database. Version 7.12.0 and all versions prior to 7.11.2 are affected.	9.8	More Details
CVE-2021-42224	SQL Injection vulnerability exists in IFSC Code Finder Project 1.0 via the searchifsccode POST parameter in /search.php.	9.8	More Details
CVE-2021-3881	libmobi is vulnerable to Out-of-bounds Read	9.8	More Details
CVE-2021-41075	The NetFlow Analyzer in Zoho ManageEngine OpManger before 125455 is vulnerable to SQL Injection in the Attacks Module API.	9.8	More Details
CVE-2021-40493	Zoho ManageEngine OpManager before 125437 is vulnerable to SQL Injection in the support diagnostics module. This occurs via the pollingObject parameter of the getDataCollectionFailureReason API.	9.8	More Details
CVE-2020-22724	A remote command execution vulnerability exists in add_server_service of PPTP_SERVER in Mercury Router MER1200 v1.0.1 and Mercury Router MER1200G v1.0.1.	9.8	More Details
CVE-2021-41132	OMERO.web provides a web based client and plugin infrastructure. In versions prior to 5.11.0, a variety of templates do not perform proper sanitization through HTML escaping. Due to the lack of sanitization and use of ``jQuery.html()``, there are a whole host of cross-site scripting possibilities with specially crafted input to a variety of fields. This issue is patched in version 5.11.0. There are no known workarounds aside from upgrading.	9.8	More Details
CVE-2021-37736	A remote authentication bypass vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	9.8	More Details
CVE-2021-3878	corenlp is vulnerable to Improper Restriction of XML External Entity Reference	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38480	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to cross-site request forgery when unauthorized commands are submitted from a user the web application trusts. This may allow an attacker to remotely perform actions on the router's management portal, such as making configuration changes, changing administrator credentials, and running system commands on the router.	9.6	More Details
CVE-2021-20599	Cleartext Transmission of Sensitive InformationCleartext transmission of sensitive information vulnerability in MELSEC iQ-R series Safety CPU R08/16/32/120SFCPU firmware versions "26" and prior and MELSEC iQ-R series SIL2 Process CPU R08/16/32/120PSFCPU firmware versions "11" and prior allows a remote unauthenticated attacker to login to a target CPU module by obtaining credentials other than password.	9.1	More Details
CVE-2021-38470	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to an attacker using a ping tool to inject commands into the device. This may allow the attacker to remotely run commands on behalf of the device.	9.1	More Details
CVE-2021-38478	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to an attacker using a traceroute tool to inject commands into the device. This may allow the attacker to remotely run commands on behalf of the device.	9.1	More Details
CVE-2021-38484	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 do not have a filter or signature check to detect or prevent an upload of malicious files to the server, which may allow an attacker, acting as an administrator, to upload malicious files. This could result in cross-site scripting, deletion of system files, and remote code execution.	9.1	More Details
CVE-2020-12141	An out-of-bounds read in the SNMP stack in Contiki-NG 4.4 and earlier allows an attacker to cause a denial of service and potentially disclose information via crafted SNMP packets to snmp_ber_decode_string_len_buffer in os/net/app-layer/snmp/snmp-ber.c.	9.1	More Details
CVE-2021-26427	Microsoft Exchange Server Remote Code Execution Vulnerability	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2021-29745	IBM Cognos Analytics 11.1.7 and 11.2.0 is vulnerable to priviledge escalation where a lower evel user could have access to the 'New Job' page to which they should not have access to. IBM X-Force ID: 201695.	8.8	More Details
CVE-2021-31372	An Improper Input Validation vulnerability in J-Web of Juniper Networks Junos OS allows a locally authenticated J-Web attacker to escalate their privileges to root over the target device. This issue affects: Juniper Networks Junos OS All versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2, 21.1R3; 21.2 versions prior to 21.2R1-S1, 21.2R2;	8.8	More Details
CVE-2021-42330	The “Teacher Edit” function of ShinHer StudyOnline System does not perform authority control. After logging in with user’s privilege, remote attackers can access and edit other users’ credential and personal information by crafting URL parameters.	8.8	More Details
CVE-2021-41148	Tuleap Open ALM is a libre and open source tool for end to end traceability of application and system developments. Prior to version 11.16.99.173 of Community Edition and versions 11.16-6 and 11.15-8 of Enterprise Edition, an attacker with the ability to add one the CI widget to its personal dashboard could execute arbitrary SQL queries. Tuleap Community Edition 11.16.99.173, Tuleap Enterprise Edition 11.16-6, and Tuleap Enterprise Edition 11.15-8 contain a patch for this issue.	8.8	More Details
CVE-2021-20831	Cross-site request forgery (CSRF) vulnerability in OG Tags versions prior to 2.0.2 allows a remote attacker to hijack the authentication of administrators and unintended operation may be performed via unspecified vectors.	8.8	More Details
CVE-2021-42333	The Easytest contains SQL injection vulnerabilities. After obtaining user’s privilege, remote attackers can inject SQL commands into the parameters of the learning history page to access all database and obtain administrator permissions.	8.8	More Details
CVE-2021-42334	The Easytest contains SQL injection vulnerabilities. After obtaining a user’s privilege, remote attackers can inject SQL commands into the parameters of the elective course management page to obtain all database and administrator permissions.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24684	The WordPress PDF Light Viewer Plugin WordPress plugin before 1.4.12 allows users with Author roles to execute arbitrary OS command on the server via OS Command Injection when invoking Ghostscript.	8.8	More Details
CVE-2021-41155	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In affected versions Tuleap does not sanitize properly user inputs when constructing the SQL query to browse and search revisions in the CVS repositories. The following versions contain the fix: Tuleap Community Edition 11.17.99.146, Tuleap Enterprise Edition 11.17-5, Tuleap Enterprise Edition 11.16-7.	8.8	More Details
CVE-2021-22964	A redirect vulnerability in the `fastify-static` module version >= 4.2.4 and < 4.4.1 allows remote attackers to redirect Mozilla Firefox users to arbitrary websites via a double slash `//` followed by a domain: `http://localhost:3000//a//youtube.com/%2e%2e%2f%2e%2e`.A DOS vulnerability is possible if the URL contains invalid characters `curl --path-as-is "http://localhost:3000//^/.."`The issue shows up on all the `fastify-static` applications that set `redirect: true` option. By default, it is `false`.	8.8	More Details
CVE-2021-41137	Minio is a Kubernetes native application for cloud storage. All users on release `RELEASE.2021-10-10T16-53-30Z` are affected by a vulnerability that involves bypassing policy restrictions on regular users. Normally, checkKeyValid() should return owner true for rootCreds. In the affected version, policy restriction did not work properly for users who did not have service (svc) or security token service (STS) accounts. This issue is fixed in `RELEASE.2021-10-13T00-23-17Z`. A downgrade back to release `RELEASE.2021-10-08T23-58-24Z` is available as a workaround.	8.8	More Details
CVE-2021-37737	A remote SQL injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	8.8	More Details
CVE-2021-20131	ManageEngine ADManager Plus Build 7111 contains a post-authentication remote code execution vulnerability due to improperly validated file uploads in the Personalization interface.	8.8	More Details
CVE-2021-20130	ManageEngine ADManager Plus Build 7111 contains a post-authentication remote code execution vulnerability due to improperly validated file uploads in the PasswordExpiry interface.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20126	Draytek VigorConnect 1.6.0-B3 lacks cross-site request forgery protections and does not sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.	8.8	More Details
CVE-2021-41154	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In affected versions an attacker with read access to a "SVN core" repository could execute arbitrary SQL queries. The following versions contain the fix: Tuleap Community Edition 11.17.99.144, Tuleap Enterprise Edition 11.17-5, Tuleap Enterprise Edition 11.16-7.	8.8	More Details
CVE-2021-38466	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 do not perform sufficient input validation on client requests from the help page. This may allow an attacker to perform a reflected cross-site scripting attack, which could allow an attacker to run code on behalf of the client browser.	8.8	More Details
CVE-2021-3858	snipe-it is vulnerable to Cross-Site Request Forgery (CSRF)	8.8	More Details
CVE-2021-20795	Cross-site request forgery (CSRF) vulnerability in the management screen of Cybozu Remote Service 3.1.8 to 3.1.9 allows a remote attacker to hijack the authentication of administrators and unintended operations may be performed via unspecified vectors.	8.8	More Details
CVE-2021-31385	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in J-Web of Juniper Networks Junos OS allows any low-privileged authenticated attacker to elevate their privileges to root. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S19; 15.1 versions prior to 15.1R7-S10; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38346	The Brizy Page Builder plugin <= 2.3.11 for WordPress allowed authenticated users to upload executable files to a location of their choice using the brizy_create_block_screenshot AJAX action. The file would be named using the id parameter, which could be prepended with "../" to perform directory traversal, and the file contents were populated via the ibsf parameter, which would be base64-decoded and written to the file. While the plugin added a .jpg extension to all uploaded filenames, a double extension attack was still possible, e.g. a file named shell.php would be saved as shell.php.jpg, and would be executable on a number of common configurations.	8.8	More Details
CVE-2021-33177	The Bulk Modifications functionality in Nagios XI versions prior to 5.8.5 is vulnerable to SQL injection. Exploitation requires the malicious actor to be authenticated to the vulnerable system, but once authenticated they would be able to execute arbitrary sql queries.	8.8	More Details
CVE-2021-3846	firefly-iii is vulnerable to Unrestricted Upload of File with Dangerous Type	8.8	More Details
CVE-2021-41971	Apache Superset up to and including 1.3.0 when configured with ENABLE_TEMPLATE_PROCESSING on (disabled by default) allowed SQL injection when a malicious authenticated user sends an http request with a custom URL.	8.8	More Details
CVE-2021-42098	An incomplete permission check on entries in Devolutions Remote Desktop Manager before 2021.2.16 allows attackers to bypass permissions via batch custom PowerShell.	8.8	More Details
CVE-2021-29679	IBM Cognos Analytics 11.1.7 and 11.2.0 could allow an authenticated user to execute code remotely due to incorrectly neutralizaing user-contrlled input that could be interpreted a a server-side include (SSI) directive. IBM X-Force ID: 199915.	8.8	More Details
CVE-2021-42228	A Cross Site Request Forgery (CSRF) vulnerability exists in KindEditor 4.1.x, as demonstrated by examples/uploadbutton.html.	8.8	More Details
CVE-2021-36970	Windows Print Spooler Spoofing Vulnerability	8.8	More Details
CVE-2021-38482	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 website used to control the router is vulnerable to stored cross-site scripting, which may allow an attacker to hijack sessions of users connected to the system.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32663	iTop is an open source web based IT Service Management tool. In affected versions an attacker can call the system setup without authentication. Given specific parameters this can lead to SSRF. This issue has been resolved in versions 2.6.5 and 2.7.5 and later	8.7	More Details
CVE-2021-38468	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to stored cross-scripting, which may allow an attacker to hijack sessions of users connected to the system.	8.7	More Details
CVE-2021-41153	The evm crate is a pure Rust implementation of Ethereum Virtual Machine. In `evm` crate `< 0.31.0`, `JUMPI` opcode's condition is checked after the destination validity check. However, according to Geth and OpenEthereum, the condition check should happen before the destination validity check. This is a **high** severity security advisory if you use `evm` crate for Ethereum mainnet. In this case, you should update your library dependency immediately to on or after `0.31.0`. This is a **low** severity security advisory if you use `evm` crate in Frontier or in a standalone blockchain, because there's no security exploit possible with this advisory. It is **not** recommended to update to on or after `0.31.0` until all the normal chain upgrade preparations have been done. If you use Frontier or other `pallet-evm` based Substrate blockchain, please ensure to update your `spec_version` before updating this. For other blockchains, please make sure to follow a hard-fork process before you update this.	8.7	More Details
CVE-2021-41150	Tough provides a set of Rust libraries and tools for using and generating the update framework (TUF) repositories. The tough library, prior to 0.12.0, does not properly sanitize delegated role names when caching a repository, or when loading a repository from the filesystem. When the repository is cached or loaded, files ending with the .json extension could be overwritten with role metadata anywhere on the system. A fix is available in version 0.12.0. No workarounds to this issue are known.	8.2	More Details
CVE-2021-41149	Tough provides a set of Rust libraries and tools for using and generating the update framework (TUF) repositories. The tough library, prior to 0.12.0, does not properly sanitize target names when caching a repository, or when saving specific targets to an output directory. When targets are cached or saved, files could be overwritten with arbitrary content anywhere on the system. A fix is available in version 0.12.0. No workarounds to this issue are known.	8.2	More Details
CVE-2021-41344	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3888	libmobi is vulnerable to Use of Out-of-range Pointer Offset	8.1	More Details
CVE-2021-40993	A remote SQL injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	8.1	More Details
CVE-2021-3889	libmobi is vulnerable to Use of Out-of-range Pointer Offset	8.1	More Details
CVE-2021-20127	An arbitrary file deletion vulnerability exists in the file delete functionality of the Html5Servlet endpoint of Draytek VigorConnect 1.6.0-B3. This allows an authenticated user to arbitrarily delete files in any location on the target operating system with root privileges.	8.1	More Details
CVE-2021-40487	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.1	More Details
CVE-2021-3057	A stack-based buffer overflow vulnerability exists in the Palo Alto Networks GlobalProtect app that enables a man-in-the-middle attacker to disrupt system processes and potentially execute arbitrary code with SYSTEM privileges. This issue impacts: GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.9 on Windows; GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.8 on Windows; GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.8 on the Universal Windows Platform; GlobalProtect app 5.3 versions earlier than GlobalProtect app 5.3.1 on Linux.	8.1	More Details
CVE-2021-32664	Combodo iTop is an open source web based IT Service Management tool. In affected versions there is a XSS vulnerability on "run query" page when logged as administrator. This has been resolved in versions 2.6.5 and 2.7.5.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41139	Anuko Time Tracker is an open source, web-based time tracking application written in PHP. When a logged on user selects a date in Time Tracker, it is being passed on via the date parameter in URI. Because of not checking this parameter for sanity in versions prior to 1.19.30.5600, it was possible to craft the URI with malicious JavaScript, use social engineering to convince logged on user to click on such link, and have the attacker-supplied JavaScript to be executed in user's browser. This issue is patched in version 1.19.30.5600. As a workaround, one may introduce `ttValidDbDateFormatDate` function as in the latest version and add a call to it within the access checks block in time.php.	8.1	More Details
CVE-2021-40464	Windows Nearby Sharing Elevation of Privilege Vulnerability	8.0	More Details
CVE-2021-31373	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3.	8.0	More Details
CVE-2021-38672	Windows Hyper-V Remote Code Execution Vulnerability	8.0	More Details
CVE-2021-40461	Windows Hyper-V Remote Code Execution Vulnerability	8.0	More Details
CVE-2021-41348	Microsoft Exchange Server Elevation of Privilege Vulnerability	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31355	A persistent cross-site scripting (XSS) vulnerability in the captive portal graphical user interface of Juniper Networks Junos OS may allow a remote authenticated user to inject web script or HTML and steal sensitive data and credentials from a web administration session, possibly tricking a follow-on administrative user to perform administrative actions on the device. This issue affects Juniper Networks Junos OS: All versions, including the following supported releases: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D220; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R1-S1, 20.2R2; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2; 21.1 versions prior to 21.1R2.	8.0	More Details
CVE-2021-38486	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 cloud portal allows for self-registration of the affected product without any requirements to create an account, which may allow an attacker to have full control over the product and execute code within the internal network to which the product is connected.	8.0	More Details
CVE-2021-30832	A memory corruption issue was addressed with improved state management. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2021-30849	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, watchOS 8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30847	This issue was addressed with improved checks. This issue is fixed in watchOS 8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30829	A URI parsing issue was addressed with improved parsing. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local user may be able to execute arbitrary files.	7.8	More Details
CVE-2021-30842	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31358	A command injection vulnerability in sftp command processing on Juniper Networks Junos OS Evolved allows an attacker with authenticated CLI access to be able to bypass configured access protections to execute arbitrary shell commands within the context of the current user. The vulnerability allows an attacker to bypass command authorization restrictions assigned to their specific user account and execute commands that are available to the privilege level for which the user is assigned. For example, a user that is in the super-user login class, but restricted to executing specific CLI commands could exploit the vulnerability to execute any other command available to an unrestricted admin user. This vulnerability does not increase the privilege level of the user, but rather bypasses any CLI command restrictions by allowing full access to the shell. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S2-EVO; 21.1 versions prior to 21.1R2-EVO; 21.2 versions prior to 21.2R1-S1-EVO, 21.2R2-EVO.	7.8	More Details
CVE-2021-31357	A command injection vulnerability in tcpdump command processing on Juniper Networks Junos OS Evolved allows an attacker with authenticated CLI access to be able to bypass configured access protections to execute arbitrary shell commands within the context of the current user. The vulnerability allows an attacker to bypass command authorization restrictions assigned to their specific user account and execute commands that are available to the privilege level for which the user is assigned. For example, a user that is in the super-user login class, but restricted to executing specific CLI commands could exploit the vulnerability to execute any other command available to an unrestricted admin user. This vulnerability does not increase the privilege level of the user, but rather bypasses any CLI command restrictions by allowing full access to the shell. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.3R2-S1-EVO; 20.4 versions prior to 20.4R2-S2-EVO; 21.1 versions prior to 21.1R2-EVO; 21.2 versions prior to 21.2R1-S1-EVO, 21.2R2-EVO.	7.8	More Details
CVE-2021-30841	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30848	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, Safari 15, iOS 15 and iPadOS 15. Processing maliciously crafted web content may lead to code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31359	A local privilege escalation vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged user to cause the Juniper DHCP daemon (jdhcpd) process to crash, resulting in a Denial of Service (DoS), or execute arbitrary commands as root. Continued processing of malicious input will repeatedly crash the system and sustain the Denial of Service (DoS) condition. Systems are only vulnerable if jdhcpd is running, which can be confirmed via the 'show system processes' command. For example: root@host# run show system processes extensive | match dhcp 26537 root -16 0 97568K 13692K RUN 0 0:01 3.71% jdhcpd This issue affects: Juniper Networks Junos OS: All versions, including the following supported releases: 15.1 versions prior to 15.1R7-S10; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S3-EVO; All versions of 21.1-EVO.	7.8	More Details
CVE-2021-31356	A command injection vulnerability in command processing on Juniper Networks Junos OS Evolved allows an attacker with authenticated CLI access to be able to bypass configured access protections to execute arbitrary shell commands within the context of the current user. The vulnerability allows an attacker to bypass command authorization restrictions assigned to their specific user account and execute commands that are available to the privilege level for which the user is assigned. For example, a user that is in the super-user login class, but restricted to executing specific CLI commands could exploit the vulnerability to execute any other command available to an unrestricted admin user. This vulnerability does not increase the privilege level of the user, but rather bypasses any CLI command restrictions by allowing full access to the shell. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S1-EVO; All versions of 21.1-EVO and 21.2-EVO.	7.8	More Details
CVE-2021-30807	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.5.1, iOS 14.7.1 and iPadOS 14.7.1, watchOS 7.6.1. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40989	A local escalation of privilege vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	7.8	More Details
CVE-2021-30830	A memory corruption issue was addressed with improved memory handling. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-40728	Adobe Acrobat Reader DC version 21.007.20095 (and earlier), 21.007.20096 (and earlier), 20.004.30015 (and earlier), and 17.011.30202 (and earlier) is affected by a use-after-free vulnerability in the processing of the GetURL function on a global object window 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.	7.8	More Details
CVE-2021-40724	Acrobat Reader for Android versions 21.8.0 (and earlier) are affected by a Path traversal vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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.	7.8	More Details
CVE-2021-30827	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2021-30838	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 15 and iPadOS 15. A malicious application may be able to execute arbitrary code with system privileges on devices with an Apple Neural Engine.	7.8	More Details
CVE-2021-30837	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8, tvOS 15. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-30835	This issue was addressed with improved checks. This issue is fixed in Security Update 2021-005 Catalina, iTunes 12.12 for Windows, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40854	AnyDesk before 6.2.6 and 6.3.x before 6.3.3 allows a local user to obtain administrator privileges by using the Open Chat Log feature to launch a privileged Notepad process that can launch other applications.	7.8	More Details
CVE-2021-3872	vim is vulnerable to Heap-based Buffer Overflow	7.8	More Details
CVE-2021-30825	This issue was addressed with improved checks. This issue is fixed in iOS 15 and iPadOS 15. A local attacker may be able to cause unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-26441	Storage Spaces Controller Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-28021	Buffer overflow vulnerability in function stbi__extend_receive in stb_image.h in stb 2.26 via a crafted JPEG file.	7.8	More Details
CVE-2021-40471	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-40480	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-41357	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-40478	Storage Spaces Controller Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-40477	Windows Event Tracing Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-38430	FATEK Automation WinProladder versions 3.30 and prior proper validation of user-supplied data when parsing project files, which could result in a stack-based buffer overflow. An attacker could leverage this vulnerability to execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38434	FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in an unexpected sign extension. An attacker could leverage this vulnerability to execute arbitrary code.	7.8	More Details
CVE-2021-40474	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-40473	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-38436	FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in a memory-corruption condition. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2021-40470	DirectX Graphics Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-40485	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-38438	A use after free vulnerability in FATEK Automation WinProladder versions 3.30 and prior may be exploited when a valid user opens a malformed project file, which may allow arbitrary code execution.	7.8	More Details
CVE-2021-38442	FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in a heap-corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-40467	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-40466	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-40465	Windows Text Shaping Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40462	Windows Media Foundation Dolby Digital Atmos Decoders Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-40450	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-40449	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-40443	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-38426	FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code.	7.8	More Details
CVE-2021-40479	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-30846	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing maliciously crafted web content may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30843	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution.	7.8	More Details
CVE-2021-40486	Microsoft Word Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-40488	Storage Spaces Controller Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-40489	Storage Spaces Controller Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41330	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-41347	Windows AppX Deployment Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-41331	Windows Media Audio Decoder Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-21797	An exploitable double-free vulnerability exists in the JavaScript implementation of Nitro Pro PDF. A specially crafted document can cause a reference to a timeout object to be stored in two different places. When closed, the document will result in the reference being released twice. This can lead to code execution under the context of the application. An attacker can convince a user to open a document to trigger this vulnerability.	7.8	More Details
CVE-2021-21796	An exploitable use-after-free vulnerability exists in the JavaScript implementation of Nitro Pro PDF. A specially crafted document can cause an object containing the path to a document to be destroyed and then later reused, resulting in a use-after-free vulnerability, which can lead to code execution under the context of the application. An attacker can convince a user to open a document to trigger this vulnerability.	7.8	More Details
CVE-2021-41335	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-41345	Storage Spaces Controller Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-41340	Windows Graphics Component Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41152	OpenOlat is a web-based e-learning platform for teaching, learning, assessment and communication, an LMS, a learning management system. In affected versions by manipulating the HTTP request an attacker can modify the path of a requested file download in the folder component to point to anywhere on the target system. The attack could be used to read any file accessible in the web root folder or outside, depending on the configuration of the system and the properly configured permission of the application server user. The attack requires an OpenOlat user account or the enabled guest user feature together with the usage of the folder component in a course. The attack does not allow writing of arbitrary files, it allows only reading of files and also only ready of files that the attacker knows the exact path which is very unlikely at least for OpenOlat data files. The problem is fixed in version 15.5.8 and 16.0.1 It is advised to upgrade to version 16.0.x. There are no known workarounds to fix this problem, an upgrade is necessary.	7.7	More Details
CVE-2021-40463	Windows Network Address Translation (NAT) Denial of Service Vulnerability	7.7	More Details
CVE-2021-40483	Microsoft SharePoint Server Spoofing Vulnerability	7.6	More Details
CVE-2021-40484	Microsoft SharePoint Server Spoofing Vulnerability	7.6	More Details
CVE-2021-36512	An issue was discovered in function scanallsubs in src/sbbs3/scansubs.cpp in Synchronet BBS, which may allow attackers to view sensitive information due to an uninitialized value.	7.5	More Details
CVE-2021-41611	An issue was discovered in Squid 5.0.6 through 5.1.x before 5.2. When validating an origin server or peer certificate, Squid may incorrectly classify certain certificates as trusted. This problem allows a remote server to obtain security trust well improperly. This indication of trust may be passed along to clients, allowing access to unsafe or hijacked services.	7.5	More Details
CVE-2021-42340	The fix for bug 63362 present in Apache Tomcat 10.1.0-M1 to 10.1.0-M5, 10.0.0-M1 to 10.0.11, 9.0.40 to 9.0.53 and 8.5.60 to 8.5.71 introduced a memory leak. The object introduced to collect metrics for HTTP upgrade connections was not released for WebSocket connections once the connection was closed. This created a memory leak that, over time, could lead to a denial of service via an OutOfMemoryError.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36389	In Yellowfin before 9.6.1 it is possible to enumerate and download uploaded images through an Insecure Direct Object Reference vulnerability exploitable by sending a specially crafted HTTP GET request to the page "MIImage.i4".	7.5	More Details
CVE-2021-3869	corenlp is vulnerable to Improper Restriction of XML External Entity Reference	7.5	More Details
CVE-2021-42261	Revisor Video Management System (VMS) before 2.0.0 has a directory traversal vulnerability. Successful exploitation could allow an attacker to traverse the file system to access files or directories that are outside of restricted directory on the remote server. This could lead to the disclosure of sensitive data on the vulnerable server.	7.5	More Details
CVE-2021-37738	A remote disclosure of sensitive information vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	7.5	More Details
CVE-2021-36388	In Yellowfin before 9.6.1 it is possible to enumerate and download users profile pictures through an Insecure Direct Object Reference vulnerability exploitable by sending a specially crafted HTTP GET request to the page "MIIAvatarImage.i4".	7.5	More Details
CVE-2021-36513	An issue was discovered in function sofia_handle_sip_i_notify in sofia.c in SignalWire freeswitch before 1.10.6, may allow attackers to view sensitive information due to an uninitialized value.	7.5	More Details
CVE-2020-29622	A race condition was addressed with additional validation. This issue is fixed in Security Update 2021-005 Catalina. Mounting a maliciously crafted NFS network share may lead to arbitrary code execution with system privileges.	7.5	More Details
CVE-2018-16060	Mitsubishi Electric Europe B.V. SmartRTU devices allow remote attackers to obtain sensitive information (directory listing and source code) via a direct request to the /web URI.	7.5	More Details
CVE-2021-30826	A logic issue was addressed with improved state management. This issue is fixed in iOS 15 and iPadOS 15. In certain situations, the baseband would fail to enable integrity and ciphering protection.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41991	The in-memory certificate cache in strongSwan before 5.9.4 has a remote integer overflow upon receiving many requests with different certificates to fill the cache and later trigger the replacement of cache entries. The code attempts to select a less-often-used cache entry by means of a random number generator, but this is not done correctly. Remote code execution might be a slight possibility.	7.5	More Details
CVE-2021-41990	The gmp plugin in strongSwan before 5.9.4 has a remote integer overflow via a crafted certificate with an RSASSA-PSS signature. For example, this can be triggered by an unrelated self-signed CA certificate sent by an initiator. Remote code execution cannot occur.	7.5	More Details
CVE-2021-38562	Best Practical Request Tracker (RT) 4.2 before 4.2.17, 4.4 before 4.4.5, and 5.0 before 5.0.2 allows sensitive information disclosure via a timing attack against lib/RT/REST2/Middleware/Auth.pm.	7.5	More Details
CVE-2021-42341	checkpath in OpenRC before 0.44.7 uses the direct output of strlen() to allocate strings, which does not account for the '\0' byte at the end of the string. This results in memory corruption. CVE-2021-42341 was introduced in git commit 63db2d99e730547339d1bdd28e8437999c380cae, which was introduced as part of OpenRC 0.44.0 development.	7.5	More Details
CVE-2021-30844	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A remote attacker may be able to leak memory.	7.5	More Details
CVE-2021-41131	python-tuf is a Python reference implementation of The Update Framework (TUF). In both clients (`tuf/client` and `tuf/ngclient`), there is a path traversal vulnerability that in the worst case can overwrite files ending in `.json` anywhere on the client system on a call to `get_one_valid_targetinfo()`. It occurs because the rolename is used to form the filename, and may contain path traversal characters (ie `../../name.json`). The impact is mitigated by a few facts: It only affects implementations that allow arbitrary rolename selection for delegated targets metadata, The attack requires the ability to A) insert new metadata for the path-traversing role and B) get the role delegated by an existing targets metadata, The written file content is heavily restricted since it needs to be a valid, signed targets file. The file extension is always .json. A fix is available in version 0.19 or newer. There are no workarounds that do not require code changes. Clients can restrict the allowed character set for rolenames, or they can store metadata in files named in a way that is not vulnerable: neither of these approaches is possible without modifying python-tuf.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41352	SCOM Information Disclosure Vulnerability	7.5	More Details
CVE-2021-31368	An Uncontrolled Resource Consumption vulnerability in the kernel of Juniper Networks JUNOS OS allows an unauthenticated network based attacker to cause 100% CPU load and the device to become unresponsive by sending a flood of traffic to the out-of-band management ethernet port. Continued receipted of a flood will create a sustained Denial of Service (DoS) condition. Once the flood subsides the system will recover by itself. An indication that the system is affected by this issue would be that kernel and netisr process are shown to be using a lot of CPU cycles like in the following example output: user@host> show system processes extensive ... PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 16 root -72 - 0K 304K WAIT 1 839:40 88.96% intr{swi1: netisr 0} 0 root 97 - 0K 160K RUN 1 732:43 87.99% kernel{bcm560xgmac0 que} This issue affects Juniper Networks JUNOS OS on EX2300 Series, EX3400 Series, and ACX710: All versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S9; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2.	7.5	More Details
CVE-2021-31374	On Juniper Networks Junos OS and Junos OS Evolved devices processing a specially crafted BGP UPDATE or KEEPALIVE message can lead to a routing process daemon (RPD) crash and restart, causing a Denial of Service (DoS). Continued receipt and processing of this message will create a sustained Denial of Service (DoS) condition. This issue affects both IBGP and EBGP deployments over IPv4 or IPv6. This issue affects: Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R1-S4, 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS Evolved: 20.3 versions prior to 20.3R2-EVO.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31376	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending specific DHCPv6 packets to the device and crashing the FXPC service. Continued receipt and processing of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms in ACX Series: ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096 devices. Other ACX platforms are not affected from this issue. This issue affects Juniper Networks Junos OS on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096: 18.4 version 18.4R3-S7 and later versions prior to 18.4R3-S8. This issue does not affect: Juniper Networks Junos OS 18.4 versions prior to 18.4R3-S7 on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096.	7.5	More Details
CVE-2021-31353	An Improper Handling of Exceptional Conditions vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an attacker to inject a specific BGP update, causing the routing protocol daemon (RPD) to crash and restart, leading to a Denial of Service (DoS). Continued receipt and processing of the BGP update will create a sustained Denial of Service (DoS) condition. This issue affects very specific versions of Juniper Networks Junos OS: 19.3R3-S2; 19.4R3-S3; 20.2 versions 20.2R2-S3 and later, prior to 20.2R3-S2; 20.3 versions 20.3R2 and later, prior to 20.3R3; 20.4 versions 20.4R2 and later, prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS 20.1 is not affected by this issue. This issue also affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S3-EVO, 20.4R3-EVO; 21.1-EVO versions prior to 21.1R2-EVO; 21.2-EVO versions prior to 21.2R2-EVO.	7.5	More Details
CVE-2021-31351	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240;	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40476	Windows AppContainer Elevation Of Privilege Vulnerability	7.5	More Details
CVE-2021-31350	An Improper Privilege Management vulnerability in the gRPC framework, used by the Juniper Extension Toolkit (JET) API on Juniper Networks Junos OS and Junos OS Evolved, allows a network-based, low-privileged authenticated attacker to perform operations as root, leading to complete compromise of the targeted system. The issue is caused by the JET service daemon (jsd) process authenticating the user, then passing configuration operations directly to the management daemon (mgd) process, which runs as root. This issue affects Juniper Networks Junos OS: 18.4 versions prior to 18.4R1-S8, 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R2-S3, 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31379	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 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 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1.	7.5	More Details
CVE-2021-0299	An Improper Handling of Exceptional Conditions vulnerability in the processing of a transit or directly received malformed IPv6 packet in Juniper Networks Junos OS results in a kernel crash, causing the device to restart, leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects systems with IPv6 configured. Devices with only IPv4 configured are not vulnerable to this issue. This issue affects Juniper Networks Junos OS: 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.4R1.	7.5	More Details
CVE-2021-34814	Proofpoint Spam Engine before 8.12.0-2106240000 has a Security Control Bypass.	7.5	More Details
CVE-2021-39304	Proofpoint Enterprise Protection before 8.12.0-2108090000 allows security control bypass.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20124	A local file inclusion vulnerability exists in Draytek VigorConnect 1.6.0-B3 in the file download functionality of the WebServlet endpoint. An unauthenticated attacker could leverage this vulnerability to download arbitrary files from the underlying operating system with root privileges.	7.5	More Details
CVE-2021-20129	An information disclosure vulnerability exists in Draytek VigorConnect 1.6.0-B3, allowing an unauthenticated attacker to export system logs.	7.5	More Details
CVE-2021-20123	A local file inclusion vulnerability exists in Draytek VigorConnect 1.6.0-B3 in the file download functionality of the DownloadFileServlet endpoint. An unauthenticated attacker could leverage this vulnerability to download arbitrary files from the underlying operating system with root privileges.	7.5	More Details
CVE-2021-31383	In Point to MultiPoint (P2MP) scenarios within established sessions between network or adjacent neighbors the improper use of a source to destination copy write operation combined with a Stack-based Buffer Overflow on certain specific packets processed by the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved sent by a remote unauthenticated network attacker causes the RPD to crash causing a Denial of Service (DoS). Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. Juniper Networks Junos OS Evolved 20.1 versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R3-EVO; 20.3 versions prior to 20.3R2-EVO.	7.5	More Details
CVE-2021-37137	The Snappy frame decoder function doesn't restrict the chunk length which may lead to excessive memory usage. Beside this it also may buffer reserved skippable chunks until the whole chunk was received which may lead to excessive memory usage as well. This vulnerability can be triggered by supplying malicious input that decompresses to a very big size (via a network stream or a file) or by sending a huge skippable chunk.	7.5	More Details
CVE-2020-19961	A SQL injection vulnerability has been discovered in zz cms version 2019 which allows attackers to retrieve sensitive data via the component subzs.php.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37933	An LDAP injection vulnerability in /account/login in Huntflow Enterprise before 3.10.6 could allow an unauthenticated, remote user to modify the logic of an LDAP query and bypass authentication. The vulnerability is due to insufficient server-side validation of the email parameter before using it to construct LDAP queries. An attacker could bypass authentication exploiting this vulnerability by sending login attempts in which there is a valid password but a wildcard character in email parameter.	7.5	More Details
CVE-2021-34453	Microsoft Exchange Server Denial of Service Vulnerability	7.5	More Details
CVE-2020-19954	An XML External Entity (XXE) vulnerability was discovered in /api/notify.php in S-CMS 3.0 which allows attackers to read arbitrary files.	7.5	More Details
CVE-2020-19957	A SQL injection vulnerability has been discovered in zz cms version 2019 which allows attackers to retrieve sensitive data via the id parameter on the /dl/dl_print.php page.	7.5	More Details
CVE-2021-37136	The Bzip2 decompression decoder function doesn't allow setting size restrictions on the decompressed output data (which affects the allocation size used during decompression). All users of Bzip2Decoder are affected. The malicious input can trigger an OOME and so a DoS attack	7.5	More Details
CVE-2020-19959	A SQL injection vulnerability has been discovered in zz cms version 2019 which allows attackers to retrieve sensitive data via the dlid parameter in the /dl/dl_sendmail.php page cookie.	7.5	More Details
CVE-2021-36953	Windows TCP/IP Denial of Service Vulnerability	7.5	More Details
CVE-2020-19960	A SQL injection vulnerability has been discovered in zz cms version 2019 which allows attackers to retrieve sensitive data via the dlid parameter in the /dl/dl_sendsms.php page cookie.	7.5	More Details
CVE-2021-0296	The Juniper Networks CTPView server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header which allows servers to indicate that content from the requested domain will only be served over HTTPS. The lack of HSTS may leave the system vulnerable to downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. This issue affects Juniper Networks CTPView: 7.3 versions prior to 7.3R7; 9.1 versions prior to 9.1R3.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20833	The SNKRDUNK Market Place App for iOS versions prior to 2.2.0 does not verify server certificate properly, which allows man-in-the-middle attackers to eavesdrop on and/or alter encrypted communication via a crafted certificate.	7.4	More Details
CVE-2021-40457	Microsoft Dynamics 365 Customer Engagement Cross-Site Scripting Vulnerability	7.4	More Details
CVE-2021-40843	Proofpoint Insider Threat Management Server contains an unsafe deserialization vulnerability in the Web Console. An attacker with write access to the local database could cause arbitrary code to execute with SYSTEM privileges on the underlying server when a Web Console user triggers retrieval of that data. When chained with a SQL injection vulnerability, the vulnerability could be exploited remotely if Web Console users click a series of maliciously crafted URLs. All versions prior to 7.11.2 are affected.	7.3	More Details
CVE-2021-38295	In Apache CouchDB, a malicious user with permission to create documents in a database is able to attach a HTML attachment to a document. If a CouchDB admin opens that attachment in a browser, e.g. via the CouchDB admin interface Fauxton, any JavaScript code embedded in that HTML attachment will be executed within the security context of that admin. A similar route is available with the already deprecated _show and _list functionality. This privilege escalation vulnerability allows an attacker to add or remove data in any database or make configuration changes. This issue affected Apache CouchDB prior to 3.1.2	7.3	More Details
CVE-2021-31375	An Improper Input Validation vulnerability in routing process daemon (RPD) of Juniper Networks Junos OS devices configured with BGP origin validation using Resource Public Key Infrastructure (RPKI), allows an attacker to send a specific BGP update which may cause RPKI policy-checks to be bypassed. This, in turn, may allow a spoofed advertisement to be accepted or propagated. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S18; 15.1 versions prior to 15.1R7-S9; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R2.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40992	A remote SQL injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2021-24754	The MainWP Child Reports WordPress plugin before 2.0.8 does not validate or sanitise the order parameter before using it in a SQL statement in the admin dashboard, leading to an SQL injection issue	7.2	More Details
CVE-2021-41147	Tuleap Open ALM is a libre and open source tool for end to end traceability of application and system developments. Prior to version 11.16.99.173 of Community Edition and versions 11.16-6 and 11.15-8 of Enterprise Edition, an attacker with admin rights in one agile dashboard service can execute arbitrary SQL queries. Tuleap Community Edition 11.16.99.173, Tuleap Enterprise Edition 11.16-6, and Tuleap Enterprise Edition 11.15-8 contain a patch for this issue.	7.2	More Details
CVE-2021-40986	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2021-40999	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2021-40988	A remote directory traversal vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2021-40987	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37739	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2021-40469	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2021-40998	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2021-30358	Mobile Access Portal Native Applications who's path is defined by the administrator with environment variables may run applications from other locations by the Mobile Access Portal Agent.	7.2	More Details
CVE-2021-31384	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in Juniper Networks Junos OS on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise protect access to J-Web. This issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1.	7.2	More Details
CVE-2021-40991	A remote disclosure of sensitive information vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2021-40481	Microsoft Office Visio Remote Code Execution Vulnerability	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31360	An improper privilege management vulnerability in the Juniper Networks Junos OS and Junos OS Evolved command-line interpreter (CLI) allows a low-privileged user to overwrite local files as root, possibly leading to a system integrity issue or Denial of Service (DoS). Depending on the files overwritten, exploitation of this vulnerability could lead to a sustained Denial of Service (DoS) condition, requiring manual user intervention to recover. Systems are only vulnerable if jdhcpd is running, which can be confirmed via the 'show system processes' command. For example: root@host# run show system processes extensive | match dhcp 26537 root -16 0 97568K 13692K RUN 0 0:01 3.71% jdhcpd This issue affects: Juniper Networks Junos OS: All versions, including the following supported releases: 15.1 versions prior to 15.1R7-S10; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S3-EVO; All versions of 21.1-EVO.	7.1	More Details
CVE-2021-38345	The Brizy Page Builder plugin <= 2.3.11 for WordPress used an incorrect authorization check that allowed any logged-in user accessing any endpoint in the wp-admin directory to modify the content of any existing post or page created with the Brizy editor. An identical issue was found by another researcher in Brizy <= 1.0.125 and fixed in version 1.0.126, but the vulnerability was reintroduced in version 1.0.127.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31354	An Out Of Bounds (OOB) access vulnerability in the handling of responses by a Juniper Agile License (JAL) Client in Juniper Networks Junos OS and Junos OS Evolved, configured in Network Mode (to use Juniper Agile License Manager) may allow an attacker to cause a partial Denial of Service (DoS), or lead to remote code execution (RCE). The vulnerability exists in the packet parsing logic on the client that processes the response from the server using a custom protocol. An attacker with control of a JAL License Manager, or with access to the local broadcast domain, may be able to spoof a new JAL License Manager and/or craft a response to the Junos OS License Client, leading to exploitation of this vulnerability. This issue only affects Junos systems configured in Network Mode. Systems that are configured in Standalone Mode (the default mode of operation for all systems) are not vulnerable to this issue. This issue affects: Juniper Networks Junos OS: 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: version 20.1R1-EVO and later versions, prior to 21.2R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1.	7.1	More Details
CVE-2021-41334	Windows Desktop Bridge Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-26442	Windows HTTP.sys Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-41342	Windows MSHTML Platform Remote Code Execution Vulnerability	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3882	LedgerSMB does not set the 'Secure' attribute on the session authorization cookie when the client uses HTTPS and the LedgerSMB server is behind a reverse proxy. By tricking a user to use an unencrypted connection (HTTP), an attacker may be able to obtain the authentication data by capturing network traffic. LedgerSMB 1.8 and newer switched from Basic authentication to using cookie authentication with encrypted cookies. Although an attacker can't access the information inside the cookie, nor the password of the user, possession of the cookie is enough to access the application as the user from which the cookie has been obtained. In order for the attacker to obtain the cookie, first of all the server must be configured to respond to unencrypted requests, the attacker must be suitably positioned to eavesdrop on the network traffic between the client and the server *and* the user must be tricked into using unencrypted HTTP traffic. Proper audit control and separation of duties limit Integrity impact of the attack vector. Users of LedgerSMB 1.8 are urged to upgrade to known-fixed versions. Users of LedgerSMB 1.7 or 1.9 are unaffected by this vulnerability and don't need to take action. As a workaround, users may configure their Apache or Nginx reverse proxy to add the Secure attribute at the network boundary instead of relying on LedgerSMB. For Apache, please refer to the 'Header always edit' configuration command in the mod_headers module. For Nginx, please refer to the 'proxy_cookie_flags' configuration command.	6.8	More Details
CVE-2021-41156	anuko/timetracker is an, open source time tracking system. In affected versions Time Tracker uses browser_today hidden control on a few pages to collect the today's date from user browsers. Because of not checking this parameter for sanity in versions prior to 1.19.30.5601, it was possible to craft an html form with malicious JavaScript, use social engineering to convince logged on users to execute a POST from such form, and have the attacker-supplied JavaScript to be executed in user's browser. This has been patched in version 1.19.30.5600. Upgrade is recommended. If it is not practical, introduce ttValidDbDateFormatDate function as in the latest version and add a call to it within the access checks block.	6.8	More Details
CVE-2021-42055	ASUSTek ZenBook Pro Due 15 UX582 laptop firmware through 203 has Insecure Permissions that allow attacks by a physically proximate attacker.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31378	In broadband environments, including but not limited to Enhanced Subscriber Management, (CHAP, PPP, DHCP, etc.), on Juniper Networks Junos OS devices where RADIUS servers are configured for managing subscriber access and a subscriber is logged in and then requests to logout, the subscriber may be forced into a "Terminating" state by an attacker who is able to send spoofed messages appearing to originate from trusted RADIUS server(s) destined to the device in response to the subscriber's request. These spoofed messages cause the Junos OS General Authentication Service (authd) daemon to force the broadband subscriber into this "Terminating" state which the subscriber will not recover from thereby causing a Denial of Service (DoS) to the endpoint device. Once in the "Terminating" state, the endpoint subscriber will no longer be able to access the network. Restarting the authd daemon on the Junos OS device will temporarily clear the subscribers out of the "Terminating" state. As long as the attacker continues to send these spoofed packets and subscribers request to be logged out, the subscribers will be returned to the "Terminating" state thereby creating a persistent Denial of Service to the subscriber. An indicator of compromise may be seen by displaying the output of "show subscribers summary". The presence of subscribers in the "Terminating" state may indicate the issue is occurring. This issue affects: Juniper Networks Junos OS 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. This issue does not affect: Juniper Networks Junos OS 12.3 version 12.3R1 and later versions; 15.1 version 15.1R1 and later versions.	6.8	More Details
CVE-2021-41151	Backstage is an open platform for building developer portals. In affected versions A malicious actor could read sensitive files from the environment where Scaffolder Tasks are run. The attack is executed by crafting a custom Scaffolder template with a `github:publish:pull-request` action and a particular source path. When the template is executed the sensitive files would be included in the published pull request. This vulnerability is mitigated by the fact that an attacker would need access to create and register templates in the Backstage catalog, and that the attack is very visible given that the exfiltration happens via a pull request. The vulnerability is patched in the `0.15.9` release of `@backstage/plugin-scaffolder-backend`.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40460	Windows Remote Procedure Call Runtime Security Feature Bypass Vulnerability	6.5	More Details
CVE-2021-0297	A vulnerability in the processing of TCP MD5 authentication in Juniper Networks Junos OS Evolved may allow a BGP or LDP session configured with MD5 authentication to succeed, even if the peer does not have TCP MD5 authentication enabled. This could lead to untrusted or unauthorized sessions being established, resulting in an impact on confidentiality or stability of the network. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.3R2-S1-EVO; 20.4 versions prior to 20.4R2-EVO; 21.1 versions prior to 21.1R2-EVO. Juniper Networks Junos OS is not affected by this issue.	6.5	More Details
CVE-2021-24675	The One User Avatar WordPress plugin before 2.3.7 does not check for CSRF when updating the Avatar in page where the [avatar_upload] shortcode is embed. As a result, attackers could make logged in user change their avatar via a CSRF attack	6.5	More Details
CVE-2021-24642	The Scroll Baner WordPress plugin through 1.0 does not have CSRF check in place when saving its settings, nor perform any sanitisation, escaping or validation on them. This could allow attackers to make logged in admin change them and could lead to RCE (via a file upload) as well as XSS	6.5	More Details
CVE-2021-31381	A configuration weakness in the JBoss Application Server (AppSvr) component of Juniper Networks SRC Series allows a remote attacker to send a specially crafted query to cause the web server to delete files which may allow the attacker to disrupt the integrity and availability of the system.	6.5	More Details
CVE-2021-33178	The Manage Backgrounds functionality within NagVis versions prior to 1.9.29 is vulnerable to an authenticated path traversal vulnerability. Exploitation of this results in a malicious actor having the ability to arbitrarily delete files on the local system.	6.5	More Details
CVE-2021-22036	VMware vRealize Orchestrator ((8.x prior to 8.6) contains an open redirect vulnerability due to improper path handling. A malicious actor may be able to redirect victim to an attacker controlled domain due to improper path handling in vRealize Orchestrator leading to sensitive information disclosure.	6.5	More Details
CVE-2020-19964	A Cross Site Request Forgery (CSRF) vulnerability was discovered in PHPMyWind 5.6 which allows attackers to create a new administrator account without authentication.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31382	On PTX1000 System, PTX10002-60C System, after upgrading to an affected release, a Race Condition vulnerability between the chassis daemon (chassisd) and firewall process (dfwd) of Juniper Networks Junos OS, may update the device's interfaces with incorrect firewall filters. This issue only occurs when upgrading the device to an affected version of Junos OS. Interfaces intended to have protections may have no protections assigned to them. Interfaces with one type of protection pattern may have alternate protections assigned to them. Interfaces intended to have no protections may have protections assigned to them. These firewall rule misassignments may allow genuine traffic intended to be stopped at the interface to propagate further, potentially causing disruptions in services by propagating unwanted traffic. An attacker may be able to take advantage of these misassignments. This issue affects Juniper Networks Junos OS on PTX1000 System: 17.2 versions 17.2R1 and later versions prior to 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R1-S1, 20.4R2. This issue does not affect Juniper Networks Junos OS prior to version 17.2R1 on PTX1000 System. This issue affects Juniper Networks Junos OS on PTX10002-60C System: 18.2 versions 18.2R1 and later versions prior to 18.4 versions prior to 18.4R3-S9; 19.1 versions later than 19.1R1 prior to 19.4 versions prior to 19.4R2-S5, 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions 20.4R1 and later versions prior to 21.1 versions prior to 21.1R2; 21.2 versions 21.2R1 and later versions prior to 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS prior to version 18.2R1 on PTX10002-60C System. This issue impacts all filter families (inet, inet6, etc.) and all loopback filters. It does not rely upon the location where a filter is set, impacting both logical and physical interfaces.	6.5	More Details
CVE-2021-24595	The Wp Cookie Choice WordPress plugin through 1.1.0 is lacking any CSRF check when saving its options, and do not escape them when outputting them in attributes. As a result, an attacker could make a logged in admin change them to arbitrary values including XSS payloads via a CSRF attack.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3746	A flaw was found in the libtpms code that may cause access beyond the boundary of internal buffers. The vulnerability is triggered by specially-crafted TPM2 command packets that then trigger the issue when the state of the TPM2's volatile state is written. The highest threat from this vulnerability is to system availability. This issue affects libtpms versions before 0.8.5, before 0.7.9 and before 0.6.6.	6.5	More Details
CVE-2021-3874	bookstack is vulnerable to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	6.5	More Details
CVE-2021-39864	Adobe Commerce versions 2.4.2-p2 (and earlier), 2.4.3 (and earlier) and 2.3.7p1 (and earlier) are affected by a cross-site request forgery (CSRF) vulnerability via a Wishlist Share Link. Successful exploitation could lead to unauthorized addition to customer cart by an unauthenticated attacker. Access to the admin console is not required for successful exploitation.	6.5	More Details
CVE-2021-40990	A remote disclosure of sensitive information vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	6.5	More Details
CVE-2021-41350	Microsoft Exchange Server Spoofing Vulnerability	6.5	More Details
CVE-2021-31362	A Protection Mechanism Failure vulnerability in RPD (routing protocol daemon) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause established IS-IS adjacencies to go down by sending a spoofed hello PDU leading to a Denial of Service (DoS) condition. Continued receipted of these spoofed PDUs will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R2-EVO; 21.1 versions prior to 21.1R2-EVO.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31363	In an MPLS P2MP environment a Loop with Unreachable Exit Condition vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause high load on RPD which in turn may lead to routing protocol flaps. If a system with sensor-based-stats enabled receives a specific LDP FEC this can lead to the above condition. Continued receipted of such an LDP FEC will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 19.2 version 19.2R2 and later versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R2. Juniper Networks Junos OS Evolved All versions prior to 20.1R2-S3-EVO; 20.3 versions prior to 20.3R1-S2-EVO.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31365	An Uncontrolled Resource Consumption vulnerability in Juniper Networks Junos OS on EX2300, EX3400 and EX4300 Series platforms allows an adjacent attacker sending a stream of layer 2 frames will trigger an Aggregated Ethernet (AE) interface to go down and thereby causing a Denial of Service (DoS). By continuously sending a stream of specific layer 2 frames an attacker will sustain the Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS EX4300 Series All versions prior to 15.1R7-S7; 16.1 versions prior to 16.1R7-S8; 17.1 versions prior to 17.1R2-S12; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10, 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-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2. Juniper Networks Junos OS EX3400 and EX4300-MP Series All versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S9, 18.4R3-S7; 19.1 versions prior to 19.1R2-S3, 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2. Juniper Networks Junos OS EX2300 Series All versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31366	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2.	6.5	More Details
CVE-2021-31367	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service (DoS) by sending genuine BGP flowspec packets which cause an FPC heap memory leak. Once having run out of memory the FPC will crash and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected.	6.5	More Details
CVE-2021-38476	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 authentication process response indicates and validates the existence of a username. This may allow an attacker to enumerate different user accounts.	6.5	More Details
CVE-2021-20796	Directory traversal vulnerability in the management screen of Cybozu Remote Service 3.1.8 allows a remote authenticated attacker to upload an arbitrary file via unspecified vectors.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31370	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2.	6.5	More Details
CVE-2021-20801	Cybozu Remote Service 3.1.8 to 3.1.9 allows a remote authenticated attacker to conduct XML External Entity (XXE) attacks and obtain the information stored in the product via unspecified vectors. This issue occurs only when using Mozilla Firefox.	6.5	More Details
CVE-2021-20836	Out-of-bounds read vulnerability in CX-Supervisor v4.0.0.13 and v4.0.0.16 allows an attacker with administrative privileges to cause information disclosure and/or arbitrary code execution by opening a specially crafted SCS project files.	6.5	More Details
CVE-2021-20804	Cybozu Remote Service 3.1.8 to 3.1.9 allows a remote authenticated attacker to cause a denial of service (DoS) condition via unspecified vectors.	6.5	More Details
CVE-2021-41332	Windows Print Spooler Information Disclosure Vulnerability	6.5	More Details
CVE-2021-24735	The Compact WP Audio Player WordPress plugin before 1.9.7 does not implement nonce checks, which could allow attackers to make a logged in admin change the "Disable Simultaneous Play" setting via a CSRF attack.	6.5	More Details
CVE-2021-38464	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 have inadequate encryption strength, which may allow an attacker to intercept the communication and steal sensitive information or hijack the session.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38344	The Brizy Page Builder plugin <= 2.3.11 for WordPress was vulnerable to stored XSS by lower-privileged users such as a subscribers. It was possible to add malicious JavaScript to a page by modifying the request sent to update the page via the brizy_update_item AJAX action and adding JavaScript to the data parameter, which would be executed in the session of any visitor viewing or previewing the post or page.	6.4	More Details
CVE-2021-38474	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 have has no account lockout policy configured for the login page of the product. This may allow an attacker to execute a brute-force password attack with no time limitation and without harming the normal operation of the user. This could allow an attacker to gain valid credentials for the product interface.	6.3	More Details
CVE-2021-40994	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	6.3	More Details
CVE-2021-40995	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x prior to 6.10.2 - - ClearPass Policy Manager 6.9.x prior to 6.9.7-HF1 - - ClearPass Policy Manager 6.8.x prior to 6.8.9-HF1. Aruba has released patches for ClearPass Policy Manager that address this security vulnerability.	6.3	More Details
CVE-2021-42227	Cross SIte Scripting (XSS) vulnerability exists in KindEditor 4.1.x via a Google search inurl:/examples/uploadbutton.html and then the .html file on the website that uses this editor (the file suffix is allowed).	6.1	More Details
CVE-2021-3863	snipe-it is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-42565	myfactory.FMS before 7.1-912 allows XSS via the UID parameter.	6.1	More Details
CVE-2021-42566	myfactory.FMS before 7.1-912 allows XSS via the Error parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8291	A link preview rendering issue in Rocket.Chat versions before 3.9 could lead to potential XSS attacks.	6.1	More Details
CVE-2021-22942	A possible open redirect vulnerability in the Host Authorization middleware in Action Pack >= 6.0.0 that could allow attackers to redirect users to a malicious website.	6.1	More Details
CVE-2021-42650	Cross Site Scripting (XSS vulnerability exists in Portainer before 2.9.1 via the node input box in Custom Templates.	6.1	More Details
CVE-2021-32569	In OSS-RC systems of the release 18B and older customer documentation browsing libraries under ALEX are subject to Cross-Site Scripting. This problem is completely resolved in new Ericsson library browsing tool ELEX used in systems like Ericsson Network Manager. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Ericsson Network Manager is a new generation OSS system which OSS-RC customers shall upgrade to	6.1	More Details
CVE-2021-33179	The general user interface in Nagios XI versions prior to 5.8.4 is vulnerable to authenticated reflected cross-site scripting. An authenticated victim, who accesses a specially crafted malicious URL, would unknowingly execute the attached payload.	6.1	More Details
CVE-2021-22963	A redirect vulnerability in the fastify-static module version < 4.2.4 allows remote attackers to redirect users to arbitrary websites via a double slash // followed by a domain: http://localhost:3000//google.com/%2e%2e.The issue shows up on all the fastify-static applications that set redirect: true option. By default, it is false.	6.1	More Details
CVE-2021-26589	A potential security vulnerability has been identified in HPE Superdome Flex Servers. The vulnerability could be remotely exploited to allow Cross Site Scripting (XSS) because the Session Cookie is missing an HttpOnly Attribute. HPE has provided a firmware update to resolve the vulnerability in HPE Superdome Flex Servers.	6.1	More Details
CVE-2021-40721	Adobe Connect version 11.2.3 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	6.1	More Details
CVE-2018-16061	Mitsubishi Electric Europe B.V. SmartRTU devices allow XSS via the username parameter or PATH_INFO to login.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24617	The GamePress WordPress plugin through 1.1.0 does not escape the op_edit POST parameter before outputting it back in multiple Game Option pages, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2021-35323	Cross Site Scripting (XSS) vulnerability exists in bludit 3-13-1 via the username in admin/login.	6.1	More Details
CVE-2021-20806	Open redirect vulnerability in Cybozu Remote Service 3.0.0 to 3.1.9 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	6.1	More Details
CVE-2011-1497	A cross-site scripting vulnerability flaw was found in the auto_link function in Rails before version 3.0.6.	6.1	More Details
CVE-2021-20807	Cross-site scripting vulnerability in the management screen of Cybozu Remote Service 3.0.0 to 3.1.9 allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-42223	Cross Site Scripting (XSS).vulnerability exists in Online DJ Booking Management System 1.0 in view-booking-detail.php.	6.1	More Details
CVE-2021-33988	Cross Site Scripting (XSS). vulnerability exists in Microweber CMS 1.2.7 via the Login form, which could let a malicious user execute Javascript by Inserting code in the request form.	6.1	More Details
CVE-2021-40732	XMP Toolkit version 2020.1 (and earlier) is affected by a null pointer dereference vulnerability that could result in leaking data from certain memory locations and causing a local denial of service in the context of the current user. User interaction is required to exploit this vulnerability in that the victim will need to open a specially crafted MXF file.	6.1	More Details
CVE-2021-20834	Improper authorization in handler for custom URL scheme vulnerability in Nike App for Android versions prior to 2.177 and Nike App for iOS versions prior to 2.177.1 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31364	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2.	5.9	More Details
CVE-2021-24752	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations.	5.7	More Details
CVE-2021-41355	.NET Core and Visual Studio Information Disclosure Vulnerability	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30811	This issue was addressed with improved checks. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8. A local attacker may be able to read sensitive information.	5.5	More Details
CVE-2021-39336	The Job Manager WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/admin-jobs.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 0.7.25. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-39337	The job-portal WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/admin/jobs_function.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 0.0.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-39335	The WpGenius Job Listing WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/src/admin/class/class-wpgenious-job-listing-options.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0.2. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-30819	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 15 and iPadOS 15. Processing a maliciously crafted USD file may disclose memory contents.	5.5	More Details
CVE-2021-39338	The MyBB Cross-Poster WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/classes/MyBBXPSettings.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-30845	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.6. A local user may be able to read kernel memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39334	The Job Board Vanila WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via the psjb_exp_in and the psjb_curr_in parameters found in the ~/job-settings.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-39332	The Business Manager WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization found throughout the plugin which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.4.5. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-30828	This issue was addressed with improved checks. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local user may be able to read arbitrary files as root.	5.5	More Details
CVE-2021-41343	Windows Fast FAT File System Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-39345	The HAL WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/wp-hal.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.1.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-30850	An access issue was addressed with improved access restrictions. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6, tvOS 15. A user may gain access to protected parts of the file system.	5.5	More Details
CVE-2021-27001	Clustered Data ONTAP versions 9.x prior to 9.5P18, 9.6P16, 9.7P16, 9.8P7 and 9.9.1P2 are susceptible to a vulnerability which could allow an authenticated privileged local attacker to arbitrarily modify Compliance-mode WORM data prior to the end of the retention period.	5.5	More Details
CVE-2021-39329	The JobBoardWP WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/includes/admin/class-metabox.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0.7. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39343	The MPL-Publisher WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/libs/PublisherController.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.30.2. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-39355	The Indeed Job Importer WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/indeed-job-importer/trunk/indeed-job-importer.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0.5. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-39344	The KJM Admin Notices WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/admin/class-kjm-admin-notices-admin.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.0.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-41338	Windows AppContainer Firewall Rules Security Feature Bypass Vulnerability	5.5	More Details
CVE-2010-2496	stonith-ng in pacemaker and cluster-glue passed passwords as commandline parameters, making it possible for local attackers to gain access to passwords of the HA stack and potentially influence its operations. This is fixed in cluster-glue 1.0.6 and newer, and pacemaker 1.1.3 and newer.	5.5	More Details
CVE-2021-40472	Microsoft Excel Information Disclosure Vulnerability	5.5	More Details
CVE-2021-38663	Windows exFAT File System Information Disclosure Vulnerability	5.5	More Details
CVE-2021-40468	Windows Bind Filter Driver Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39349	The Author Bio Box WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/includes/admin/class-author-bio-box-admin.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 3.3.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2021-40454	Rich Text Edit Control Information Disclosure Vulnerability	5.5	More Details
CVE-2021-38662	Windows Fast FAT File System Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-41320	A technical user has hardcoded credentials in Wallstreet Suite TRM 7.4.83 (64-bit edition) with higher privilege than the average authenticated user. NOTE: the vendor disputes this because the password is not hardcoded (it can be changed during installation or at any later time).	5.5	More Details
CVE-2021-40475	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-31377	An Incorrect Permission Assignment for Critical Resource vulnerability of a certain file in the filesystem of Junos OS allows a local authenticated attacker to cause routing process daemon (RPD) to crash and restart, causing a Denial of Service (DoS). Repeated actions by the attacker will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S7; 19.1 versions prior to 19.1R2-S3, 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R1-S1, 20.4R2.	5.5	More Details
CVE-2021-40455	Windows Installer Spoofing Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41336	Windows Kernel Information Disclosure Vulnerability	5.5	More Details
CVE-2021-3875	vim is vulnerable to Heap-based Buffer Overflow	5.5	More Details
CVE-2021-24760	The Gutenberg PDF Viewer Block WordPress plugin before 1.0.1 does not sanitise and escape its block, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2021-32609	Apache Superset up to and including 1.1 does not sanitize titles correctly on the Explore page. This allows an attacker with Explore access to save a chart with a malicious title, injecting html (including scripts) into the page.	5.4	More Details
CVE-2021-24615	The Wechat Reward WordPress plugin through 1.7 does not sanitise or escape its QR settings, nor has any CSRF check in place, allowing attackers to make a logged in admin change the settings and perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2020-19962	A stored cross-site scripting (XSS) vulnerability in the getClientIp function in /lib/tinwin.class.php of Chaoji CMS 2.39, allows attackers to execute arbitrary web scripts.	5.4	More Details
CVE-2021-41354	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2021-29912	IBM Security Risk Manager on CP4S 1.7.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 207828.	5.4	More Details
CVE-2021-3879	snipe-it is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-24672	The One User Avatar WordPress plugin before 2.3.7 does not escape the link and target attributes of its shortcode, allowing users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2021-24743	The Podcast Subscribe Buttons WordPress plugin before 1.4.2 allows users with any role capable of editing or adding posts to perform stored XSS.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41361	Active Directory Federation Server Spoofing Vulnerability	5.4	More Details
CVE-2021-20128	The Profile Name field in the floor plan (Network Menu) page in Draytek VigorConnect 1.6.0-B3 was found to be vulnerable to stored XSS, as user input is not properly sanitized.	5.4	More Details
CVE-2021-20797	Cross-site script inclusion vulnerability in the management screen of Cybozu Remote Service 3.1.8 allows a remote authenticated attacker to obtain the information stored in the product. This issue occurs only when using Mozilla Firefox.	5.4	More Details
CVE-2021-24734	The Compact WP Audio Player WordPress plugin before 1.9.7 does not escape some of its shortcodes attributes, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2021-20805	Cross-site scripting vulnerability in the management screen of Cybozu Remote Service 3.1.7 to 3.1.9 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	5.4	More Details
CVE-2021-20803	Operation restriction bypass in the management screen of Cybozu Remote Service 3.1.8 to 3.1.9 allows a remote authenticated attacker to alter the data of the management screen.	5.4	More Details
CVE-2021-20800	Cross-site scripting vulnerability in the management screen of Cybozu Remote Service 3.1.8 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	5.4	More Details
CVE-2021-29878	IBM Business Automation Workflow 18.0, 19.0, 20.0, and 21.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 206581.	5.4	More Details
CVE-2021-20799	Cross-site scripting vulnerability in the management screen of Cybozu Remote Service 3.1.8 to 3.1.9 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	5.4	More Details
CVE-2021-41353	Microsoft Dynamics 365 (on-premises) Spoofing Vulnerability	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24415	The Polo Video Gallery – Best wordpress video gallery plugin WordPress plugin through 1.2 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode	5.4	More Details
CVE-2021-24413	The Easy Twitter Feed WordPress plugin before 1.2 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode	5.4	More Details
CVE-2021-3851	firefly-iii is vulnerable to URL Redirection to Untrusted Site	5.4	More Details
CVE-2021-41142	Tuleap Open ALM is a libre and open source tool for end to end traceability of application and system developments. There is a cross-site scripting vulnerability in Tuleap Community Edition prior to 12.11.99.25 and Tuleap Enterprise Edition 12.11-2. A malicious user with the capability to add and remove attachment to an artifact could force a victim to execute uncontrolled code. Tuleap Community Edition 11.17.99.146 and Tuleap Enterprise Edition 12.11-2 contain a fix for the issue.	5.4	More Details
CVE-2021-24732	The PDF Flipbook, 3D Flipbook WordPress – DearFlip WordPress plugin before 1.7.10 does not escape the class attribute of its shortcode before outputting it back in an attribute, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2021-24412	The Html5 Audio Player – Audio Player for WordPress plugin before 2.1.3 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode	5.4	More Details
CVE-2021-36387	In Yellowfin before 9.6.1 there is a Stored Cross-Site Scripting vulnerability in the video embed functionality exploitable through a specially crafted HTTP POST request to the page "ActivityStreamAjax.i4".	5.4	More Details
CVE-2021-25968	In “OpenCMS”, versions 10.5.0 to 11.0.2 are affected by a stored XSS vulnerability that allows low privileged application users to store malicious scripts in the Sitemap functionality. These scripts are executed in a victim’s browser when they open the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42329	The “List_Add” function of message board of ShinHer StudyOnline System does not filter special characters in the title parameter. After logging in with user’s privilege, remote attackers can inject JavaScript and execute stored XSS attacks.	5.4	More Details
CVE-2021-42331	The “Study Edit” function of ShinHer StudyOnline System does not perform permission control. After logging in with user’s privilege, remote attackers can access and edit other users’ tutorial schedule by crafting URL parameters.	5.4	More Details
CVE-2021-20798	Cross-site scripting vulnerability in the management screen of Cybozu Remote Service 3.1.8 to 3.1.9 allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	5.4	More Details
CVE-2021-42335	Easytest bulletin board management function of online learning platform does not filter special characters. After obtaining a user’s privilege, remote attackers can inject JavaScript and execute stored XSS attack.	5.4	More Details
CVE-2021-24416	The StreamCast – Radio Player for WordPress plugin before 2.1.1 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode	5.4	More Details
CVE-2021-24677	The Find My Blocks WordPress plugin before 3.4.0 does not have authorisation checks in its REST API, which could allow unauthenticated users to enumerate private posts' titles.	5.3	More Details
CVE-2021-20832	InBody App for iOS versions prior to 2.3.30 and InBody App for Android versions prior to 2.2.90(510) contain a vulnerability which may lead to information disclosure only when it works with the body composition analyzer InBody Dial. This may allow an attacker who can connect to the InBody Dial with InBody App may obtain a victim's measurement result measured by InBody Dial.	5.3	More Details
CVE-2021-40482	Microsoft SharePoint Server Information Disclosure Vulnerability	5.3	More Details
CVE-2021-31352	An Information Exposure vulnerability in Juniper Networks SRC Series devices configured for NETCONF over SSH permits the negotiation of weak ciphers, which could allow a remote attacker to obtain sensitive information. A remote attacker with read and write access to network data could exploit this vulnerability to display plaintext bits from a block of ciphertext and obtain sensitive information. This issue affects all Juniper Networks SRC Series versions prior to 4.13.0-R6.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20802	HTTP header injection vulnerability in Cybozu Remote Service 3.1.8 to 3.1.9 allows a remote attacker to alter the information stored in the product.	5.3	More Details
CVE-2021-31380	A configuration weakness in the JBoss Application Server (AppSvr) component of Juniper Networks SRC Series allows a remote attacker to send a specially crafted query to cause the web server to disclose sensitive information in the HTTP response which allows the attacker to obtain sensitive information.	5.3	More Details
CVE-2021-31386	A Protection Mechanism Failure vulnerability in the J-Web HTTP service of Juniper Networks Junos OS allows a remote unauthenticated attacker to perform Person-in-the-Middle (PitM) attacks against the device. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S20; 15.1 versions prior to 15.1R7-S11; 18.3 versions prior to 18.3R3-S6; 18.4 versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2.	5.3	More Details
CVE-2021-31361	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31371	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It was discovered that packets utilizing these IP addresses may egress an QFX5000 Series switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information exposure vulnerability. This issue affects Juniper Networks Junos OS on QFX5110, QFX5120, QFX5200, QFX5210 Series, and QFX5100 with QFX 5e Series image installed: All versions prior to 17.3R3-S12; 18.1 versions prior to 18.1R3-S13; 18.3 versions prior to 18.3R3-S5; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2;	5.3	More Details
CVE-2021-41140	Discourse-reactions is a plugin for the Discourse platform that allows user to add their reactions to the post. In affected versions reactions given by user to secure topics and private messages are visible. This issue is patched in version 0.2 of discourse-reaction. Users who are unable to update are advised to disable the Discourse-reactions plugin in admin panel.	5.3	More Details
CVE-2021-31369	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41138	Frontier is Substrate's Ethereum compatibility layer. In the newly introduced signed Frontier-specific extrinsic for `pallet-ethereum`, a large part of transaction validation logic was only called in transaction pool validation, but not in block execution. Malicious validators can take advantage of this to put invalid transactions into a block. The attack is limited in that the signature is always validated, and the majority of the validation is done again in the subsequent `pallet-evm` execution logic. However, do note that a chain ID replay attack was possible. In addition, spamming attacks are of main concerns, while they are limited by Substrate block size limits and other factors. The issue is patched in commit `146bb48849e5393004be5c88beefe76fdf009aba`.	5.3	More Details
CVE-2021-41346	Console Window Host Security Feature Bypass Vulnerability	5.3	More Details
CVE-2021-40456	Windows AD FS Security Feature Bypass Vulnerability	5.3	More Details
CVE-2021-41337	Active Directory Security Feature Bypass Vulnerability	4.9	More Details
CVE-2021-38911	IBM Security Risk Manager on CP4S 1.7.0.0 stores user credentials in plain clear text which can be read by a an authenticatedl privileged user. IBM X-Force ID: 209940.	4.9	More Details
CVE-2021-32571	In OSS-RC systems of the release 18B and older during data migration procedures certain files containing usernames and passwords are left in the system undeleted but in folders accessible by top privileged accounts only. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Ericsson Network Manager is a new generation OSS system which OSS-RC customers shall upgrade to	4.9	More Details
CVE-2021-24702	The LearnPress WordPress plugin before 4.1.3.1 does not properly sanitize or escape various inputs within course settings, which could allow high privilege users to perform Cross-Site Scripting attacks when the unfiltred_html capability is disallowed	4.8	More Details
CVE-2021-24736	The Easy Download Manager and File Sharing Plugin with frontend file upload – a better Media Library — Shared Files WordPress plugin before 1.6.57 does not sanitise and escape some of its settings before outputting them in attributes, which could lead to Stored Cross-Site Scripting issues.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24740	The Tutor LMS WordPress plugin before 1.9.9 does not escape some of its settings before outputting them in attributes, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-36832	WordPress Popups, Welcome Bar, Optins and Lead Generation Plugin – Icegram (versions <= 2.0.2) vulnerable at "Headline" (&message_data[16][headline]) input.	4.8	More Details
CVE-2021-24622	The Customer Service Software & Support Ticket System WordPress plugin before 5.10.4 does not sanitize or escape form fields before outputting it in the List, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24612	The Sociable WordPress plugin through 4.3.4.1 does not sanitise or escape some of its settings before outputting them in the admins dashboard, allowing high privilege users to perform Cross-Site Scripting attacks against other users even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24516	The PlanSo Forms WordPress plugin through 2.6.3 does not escape the title of its Form before outputting it in attributes, allowing high privilege users such as admin to set XSS payload in it, even when the unfiltered_html is disallowed, leading to an Authenticated Stored Cross-Site Scripting issue.	4.8	More Details
CVE-2021-0298	A Race Condition in the 'show chassis pic' command in Juniper Networks Junos OS Evolved may allow an attacker to crash the port interface concentrator daemon (picd) process on the FPC, if the command is executed coincident with other system events outside the attacker's control, leading to a Denial of Service (DoS) condition. Continued execution of the CLI command, under precise conditions, could create a sustained Denial of Service (DoS) condition. This issue affects all Juniper Networks Junos OS Evolved versions prior to 20.1R2-EVO on PTX10003 and PTX10008 platforms. Junos OS is not affected by this vulnerability.	4.7	More Details
CVE-2021-26318	A timing and power-based side channel attack leveraging the x86 PREFETCH instructions on some AMD CPUs could potentially result in leaked kernel address space information.	4.7	More Details
CVE-2021-38472	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 management portal does not contain an X-FRAME-OPTIONS header, which an attacker may take advantage of by sending a link to an administrator that frames the router’s management portal and could lure the administrator to perform changes.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41339	Microsoft DWM Core Library Elevation of Privilege Vulnerability	4.7	More Details
CVE-2021-30810	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8, tvOS 15. An attacker in physical proximity may be able to force a user onto a malicious Wi-Fi network during device setup.	4.3	More Details
CVE-2021-3454	Truncated L2CAP K-frame causes assertion failure. Zephyr versions >= 2.4.0, >= v.2.50 contain Improper Handling of Length Parameter Inconsistency (CWE-130), Reachable Assertion (CWE-617). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-fx88-6c29-vrp3	4.3	More Details
CVE-2021-33609	Missing check in DataCommunicator class in com.vaadin:vaadin-server versions 8.0.0 through 8.14.0 (Vaadin 8.0.0 through 8.14.0) allows authenticated network attacker to cause heap exhaustion by requesting too many rows of data.	4.3	More Details
CVE-2021-3455	Disconnecting L2CAP channel right after invalid ATT request leads freeze. Zephyr versions >= 2.4.0, >= 2.5.0 contain Use After Free (CWE-416). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-7g38-3x9v-v7vp	4.3	More Details
CVE-2021-38431	An authenticated user using Advantech WebAccess SCADA in versions 9.0.3 and prior can use API functions to disclose project names and paths from other users.	4.3	More Details
CVE-2021-42336	The learning history page of the Easytest is vulnerable by permission bypass. After obtaining a user’s permission, remote attackers can access other users’ and administrator’s account information except password by crafting URL parameters.	4.3	More Details
CVE-2021-42332	The “List View” function of ShinHer StudyOnline System is not under authority control. After logging in with user’s privilege, remote attackers can access the content of other users’ message boards by crafting URL parameters.	4.3	More Details
CVE-2021-22035	VMware vRealize Log Insight (8.x prior to 8.6) contains a CSV(Comma Separated Value) injection vulnerability in interactive analytics export function. An authenticated malicious actor with non-administrative privileges may be able to embed untrusted data prior to exporting a CSV sheet through Log Insight which could be executed in user's environment.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41363	Intune Management Extension Security Feature Bypass Vulnerability	4.2	More Details
CVE-2011-1075	FreeBSD's crontab calculates the MD5 sum of the previous and new cronjob to determine if any changes have been made before copying the new version in. In particular, it uses the MD5File() function, which takes a pathname as an argument, and is called with euid 0. A race condition in this process may lead to an arbitrary MD5 comparison regardless of the read permissions.	3.7	More Details
CVE-2021-36097	Agents are able to lock the ticket without the "Owner" permission. Once the ticket is locked, it could be moved to the queue where the agent has "rw" permissions and gain a full control. This issue affects: OTRS AG OTRS 8.0.x version: 8.0.16 and prior versions.	3.5	More Details
CVE-2020-4951	IBM Cognos Analytics 11.1.7 and 11.2.0 contains locally cached browser data, that could allow a local attacker to obtain sensitive information.	3.3	More Details
CVE-2021-38440	FATEK Automation WinProladder versions 3.30 and prior is vulnerable to an out-of-bounds read, which may allow an attacker to read unauthorized information.	3.3	More Details
CVE-2021-40729	Adobe Acrobat Reader DC version 21.007.20095 (and earlier), 21.007.20096 (and earlier), 20.004.30015 (and earlier), and 17.011.30202 (and earlier) is affected by a out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious PDF file.	3.3	More Details
CVE-2021-22033	Releases prior to VMware vRealize Operations 8.6 contain a Server Side Request Forgery (SSRF) vulnerability.	2.7	More Details
CVE-2021-30815	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. This issue is fixed in iOS 15 and iPadOS 15. A local attacker may be able to view contacts from the lock screen.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40730	Adobe Acrobat Reader DC version 21.007.20095 (and earlier), 21.007.20096 (and earlier), 20.004.30015 (and earlier), and 17.011.30202 (and earlier) is affected by a use-after-free that allow a remote attacker to disclose sensitive information on affected installations of of Adobe Acrobat Reader DC. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPG2000 images.	N/A	More Details
CVE-2021-40731	Adobe Acrobat Reader DC version 21.007.20095 (and earlier), 21.007.20096 (and earlier), 20.004.30015 (and earlier), and 17.011.30202 (and earlier) is affected by an out-of-bounds write vulnerability when parsing a crafted JPEG2000 file, which 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.	N/A	More Details
CVE-2021-39330	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-24608. Reason: This candidate is a duplicate of CVE-2021-24608. Notes: All CVE users should reference CVE-2021-24608 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-3755	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