SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 15 September 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-2021-39296	In OpenBMC 2.9, crafted IPMI messages allow an attacker to bypass authentication and gain full control of the system.	10.0	More Details
CVE-2021-37181	A vulnerability has been identified in Cerberus DMS V4.0 (All versions), Cerberus DMS V4.1 (All versions), Cerberus DMS V4.2 (All versions), Cerberus DMS V5.0 (All versions < v5.0 QU1), Desigo CC Compact V4.0 (All versions), Desigo CC Compact V4.1 (All versions), Desigo CC Compact V4.2 (All versions), Desigo CC Compact V5.0 (All versions < V5.0 QU1), Desigo CC V4.0 (All versions), Desigo CC V4.1 (All versions), Desigo CC V4.2 (All versions), Desigo CC V5.0 (All versions < V5.0 QU1). The application deserialises untrusted data without sufficient validations, that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system. The CCOM communication component used for Windows App / Click-Once and IE Web / XBAP client connectivity are affected by the vulnerability.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31891	A vulnerability has been identified in Desigo CC (All versions with OIS Extension Module), GMA-Manager (All versions with OIS running on Debian 9 or earlier), Operation Scheduler (All versions with OIS running on Debian 9 or earlier), Siveillance Control (All versions with OIS running on Debian 9 or earlier), Siveillance Control Pro (All versions). The affected application incorrectly neutralizes special elements in a specific HTTP GET request which could lead to command injection. An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary code on the system with root privileges.	10.0	More Details
CVE-2021-23031	On version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3, 14.1.x before 14.1.4.1, 13.1.x before 13.1.4, 12.1.x before 12.1.6, and 11.6.x before 11.6.5.3, an authenticated user may perform a privilege escalation on the BIG-IP Advanced WAF and ASM Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	9.9	More Details
CVE-2021-38163	SAP NetWeaver (Visual Composer 7.0 RT) versions - 7.30, 7.31, 7.40, 7.50, without restriction, an attacker authenticated as a non-administrative user can upload a malicious file over a network and trigger its processing, which is capable of running operating system commands with the privilege of the Java Server process. These commands can be used to read or modify any information on the server or shut the server down making it unavailable.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32724	check-spelling is a github action which provides CI spell checking. In affected versions and for a repository with the [check-spelling action](https://github.com/marketplace/actions/check-spelling) enabled that triggers on `pull_request_target` (or `schedule`), an attacker can send a crafted Pull Request that causes a `GITHUB_TOKEN` to be exposed. With the `GITHUB_TOKEN`, it's possible to push commits to the repository bypassing standard approval processes. Commits to the repository could then steal any/all secrets available to the repository. As a workaround users may can either: [Disable the workflow](https://docs.github.com/en/actions/managing-workflow-runs/disabling-and-enabling-a-workflow) until you've fixed all branches or Set repository to [Allow specific actions](https://docs.github.com/en/github/administering-a-repository/managing-repository-settings/disabling-or-limiting-github-actions-for-a-repository#allowing-specific-actions-to-run). check-spelling isn't a verified creator and it certainly won't be anytime soon. You could then explicitly add other actions that your repository uses. Set repository [Workflow permissions](https://docs.github.com/en/github/administering-a-repository/managing-repository-settings/disabling-or-limiting-github-actions-for-a-repository#setting-the-permissions-of-the-github_token-for-your-repository) to `Read repository contents permission`. Workflows using `check-spelling/check-spelling@main` will get the fix automatically. Workflows using a pinned sha or tagged version will need to change the affected workflows for all repository branches to the latest version. Users can verify who and which Pull Requests have been running the action by looking up the spelling.yml action in the Actions tab of their repositories, e.g., https://github.com/check-spelling/check-spelling/actions/workflows/spelling.yml - you can filter PRs by adding ?query=event%3Apull_request_target, e.g., https://github.com/check-spelling/check-spelling/actions/workflows/spelling.yml?query=event%3Apull_request_target.	9.9	More Details
CVE-2021-32835	Eclipse Keti is a service that was designed to protect RESTfuls API using Attribute Based Access Control (ABAC). In Keti a sandbox escape vulnerability may lead to post-authentication Remote Code execution. This vulnerability is known to exist in the latest commit at the time of writing this CVE (commit a1c8dbe). For more details see the referenced GHSL-2021-063.	9.9	More Details
CVE-2021-3645	merge is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37422	Zoho ManageEngine ADSelfService Plus 6111 and prior is vulnerable to SQL Injection while linking the databases.	9.8	More Details
CVE-2021-37423	Zoho ManageEngine ADSelfService Plus 6111 and prior is vulnerable to linked applications takeover.	9.8	More Details
CVE-2021-40373	playSMS before 1.4.5 allows Arbitrary Code Execution by entering PHP code at the #tabs-information-page of core_main_config, and then executing that code via the index.php?app=main&inc=core_welcome URI.	9.8	More Details
CVE-2021-34345	A stack buffer overflow vulnerability has been reported to affect QNAP device running NVR Storage Expansion. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of NVR Storage Expansion: NVR Storage Expansion 1.0.6 (2021/08/03) and later	9.8	More Details
CVE-2021-34346	A stack buffer overflow vulnerability has been reported to affect QNAP device running NVR Storage Expansion. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of NVR Storage Expansion: NVR Storage Expansion 1.0.6 (2021/08/03) and later	9.8	More Details
CVE-2021-24040	Due to use of unsafe YAML deserialization logic, an attacker with the ability to modify local YAML configuration files could provide malicious input, resulting in remote code execution or similar risks. This issue affects ParlAI prior to v1.1.0.	9.8	More Details
CVE-2021-34344	A stack buffer overflow vulnerability has been reported to affect QNAP device running QUSBCam2. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QUSBCam2: QTS 4.5.4: QUSBCam2 1.1.4 (2021/07/30) and later QTS 5.0: QUSBCam2 2.0.1 (2021/08/03) and later QTS 4.3.6: QUSBCam2 1.1.4 (2021/07/30) and later QTS 4.3.3: QUSBCam2 1.1.4 (2021/08/06) and later QuTS hero 4.5.3: QUSBCam2 1.1.4 (2021/07/30) and later	9.8	More Details
CVE-2021-28911	BAB TECHNOLOGIE GmbH eibPort V3 prior version 3.9.1 allow unauthenticated attackers access to /tmp path which contains some sensitive data (e.g. device serial number). Having those info, a possible loginId can be self-calculated in a brute force attack against BMX interface. This is usable and part of an attack chain to gain SSH root access.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40864	The Translate plugin 6.1.x through 6.3.x before 6.3.0.72 for ONLYOFFICE Document Server lacks escape calls for the msg.data and text fields.	9.8	More Details
CVE-2021-40866	Certain NETGEAR smart switches are affected by a remote admin password change by an unauthenticated attacker via the (disabled by default) /sqfs/bin/sccd daemon, which fails to check authentication when the authentication TLV is missing from a received NSDP packet. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	9.8	More Details
CVE-2021-40146	A Remote Code Execution (RCE) vulnerability was discovered in the Any23 YAMLExtractor.java file and is known to affect Any23 versions < 2.5. RCE vulnerabilities allow a malicious actor to execute any code of their choice on a remote machine over LAN, WAN, or internet. RCE belongs to the broader class of arbitrary code execution (ACE) vulnerabilities.	9.8	More Details
CVE-2020-19267	An issue in index.php/Dswjcms/Basis/resources of Dswjcms 1.6.4 allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details
CVE-2021-40870	An issue was discovered in Aviatrix Controller 6.x before 6.5-1804.1922. Unrestricted upload of a file with a dangerous type is possible, which allows an unauthenticated user to execute arbitrary code via directory traversal.	9.8	More Details
CVE-2021-24493	The shopp_upload_file AJAX action of the Shopp WordPress plugin through 1.4, available to both unauthenticated and authenticated user does not have any security measure in place to prevent upload of malicious files, such as PHP, allowing unauthenticated users to upload arbitrary files and leading to RCE	9.8	More Details
CVE-2021-33543	Multiple camera devices by UDP Technology, Geutebrück and other vendors allow unauthenticated remote access to sensitive files due to default user authentication settings. This can lead to manipulation of the device and denial of service.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3666	body-parser-xml is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	9.8	More Details
CVE-2021-38833	SQL injection vulnerability in PHPGurukul Apartment Visitors Management System (AVMS) v. 1.0 allows attackers to execute arbitrary SQL statements and to gain RCE.	9.8	More Details
CVE-2021-27391	A vulnerability has been identified in APOGEE MBC (PPC) (P2 Ethernet) (All versions >= V2.6.3), APOGEE MEC (PPC) (P2 Ethernet) (All versions >= V2.6.3), APOGEE PXC Compact (BACnet) (All versions < V3.5.3), APOGEE PXC Compact (P2 Ethernet) (All versions >= V2.8), APOGEE PXC Modular (BACnet) (All versions < V3.5.3), APOGEE PXC Modular (P2 Ethernet) (All versions >= V2.8), TALON TC Compact (BACnet) (All versions < V3.5.3), TALON TC Modular (BACnet) (All versions < V3.5.3). The web server of affected devices lacks proper bounds checking when parsing the Host parameter in HTTP requests, which could lead to a buffer overflow. An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary code on the device with root privileges.	9.8	More Details
CVE-2021-33719	A vulnerability has been identified in SIPROTEC 5 relays with CPU variants CP050 (All versions < V8.80), SIPROTEC 5 relays with CPU variants CP100 (All versions < V8.80), SIPROTEC 5 relays with CPU variants CP300 (All versions < V8.80). Specially crafted packets sent to port 4443/tcp could cause a Denial-of-Service condition or potential remote code execution.	9.8	More Details
CVE-2021-37184	A vulnerability has been identified in Industrial Edge Management (All versions < V1.3). An unauthenticated attacker could change the the password of any user in the system under certain circumstances. With this an attacker could impersonate any valid user on an affected system.	9.8	More Details
CVE-2021-36581	Kooboo CMS 2.1.1.0 is vulnerable to Insecure file upload. It is possible to upload any file extension to the server. The server does not verify the extension of the file and the tester was able to upload an aspx to the server.	9.8	More Details
CVE-2021-36582	In Kooboo CMS 2.1.1.0, it is possible to upload a remote shell (e.g., aspx) to the server and then call upon it to receive a reverse shell from the victim server. The files are uploaded to /Content/Template/root/reverse-shell.aspx and can be simply triggered by browsing that URL.	9.8	More Details
CVE-2021-37535	SAP NetWeaver Application Server Java (JMS Connector Service) - versions 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not perform necessary authorization checks for user privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28909	BAB TECHNOLOGIE GmbH eibPort V3 prior version 3.9.1 allow unauthenticated attackers to access uncontrolled the login service at /webif/SecurityModule in a brute force attack. The password could be weak and default username is known as 'admin'. This is usable and part of an attack chain to gain SSH root access.	9.8	More Details
CVE-2020-19853	BlueCMS v1.6 contains a SQL injection vulnerability via /ad_js.php.	9.8	More Details
CVE-2021-38727	FUEL CMS 1.5.0 allows SQL Injection via parameter 'col' in /fuel/index.php/fuel/logs/items	9.8	More Details
CVE-2020-24672	A vulnerability in Base Software for SoftControl allows an attacker to insert and run arbitrary code in a computer running the affected product. This issue affects: .	9.8	More Details
CVE-2021-1916	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2021-1919	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2021-1920	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2021-1972	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2021-30793	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. An application may be able to execute arbitrary code with kernel privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30805	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. An application may be able to execute arbitrary code with kernel privileges.	9.8	More Details
CVE-2021-1770	A buffer overflow may result in arbitrary code execution. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. A logic issue was addressed with improved state management.	9.8	More Details
CVE-2021-1829	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.3. An application may be able to execute arbitrary code with kernel privileges.	9.8	More Details
CVE-2021-1834	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave. A malicious application may be able to execute arbitrary code with kernel privileges.	9.8	More Details
CVE-2021-1864	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. An attacker with JavaScript execution may be able to execute arbitrary code.	9.8	More Details
CVE-2021-1882	A memory corruption issue was addressed with improved validation. This issue is fixed in Security Update 2021-002 Catalina, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. An application may be able to gain elevated privileges.	9.8	More Details
CVE-2021-30655	An application may be able to execute arbitrary code with system privileges. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina. The issue was addressed with improved permissions logic.	9.8	More Details
CVE-2021-38540	The variable import endpoint was not protected by authentication in Airflow >=2.0.0, <2.1.3. This allowed unauthenticated users to hit that endpoint to add/modify Airflow variables used in DAGs, potentially resulting in a denial of service, information disclosure or remote code execution. This issue affects Apache Airflow >=2.0.0, <2.1.3.	9.8	More Details
CVE-2021-30690	Multiple issues in apache were addressed by updating apache to version 2.4.46. This issue is fixed in Security Update 2021-004 Mojave. Multiple issues in apache.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30678	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	9.8	More Details
CVE-2021-28913	BAB TECHNOLOGIE GmbH eibPort V3 prior version 3.9.1 allow unauthenticated attackers access to /webif/SecurityModule to validate the so called and hard coded unique 'eibPort String' which acts as the root SSH key passphrase. This is usable and part of an attack chain to gain SSH root access.	9.8	More Details
CVE-2020-26772	Command Injection in PPGo_Jobs v2.8.0 allows remote attackers to execute arbitrary code via the 'AjaxRun()' function.	9.8	More Details
CVE-2021-36440	Unrestricted File Upload in ShowDoc v2.9.5 allows remote attackers to execute arbitrary code via the 'file_url' parameter in the component AdminUpdateController.class.php'.	9.8	More Details
CVE-2021-40814	The Customer Photo Gallery addon before 2.9.4 for PrestaShop is vulnerable to SQL injection.	9.8	More Details
CVE-2021-40818	scheme/webauthn.c in Glewlwyd SSO server through 2.5.3 has a buffer overflow during FIDO2 signature validation in webauthn registration.	9.8	More Details
CVE-2021-1933	UE assertion is possible due to improper validation of invite message with SDP body in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	9.8	More Details
CVE-2021-1946	Null Pointer Dereference may occur due to improper validation while processing crafted SDP body in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	9.8	More Details
CVE-2021-36161	Some component in Dubbo will try to print the formated string of the input arguments, which will possibly cause RCE for a maliciously customized bean with special toString method. In the latest version, we fix the toString call in timeout, cache and some other places. Fixed in Apache Dubbo 2.7.13	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37579	The Dubbo Provider will check the incoming request and the corresponding serialization type of this request meet the configuration set by the server. But there's an exception that the attacker can use to skip the security check (when enabled) and reaching a deserialization operation with native java serialization. Apache Dubbo 2.7.13, 3.0.2 fixed this issue by quickly fail when any unrecognized request was found.	9.8	More Details
CVE-2020-19138	Unrestricted Upload of File with Dangerous Type in DotCMS v5.2.3 and earlier allow remote attackers to execute arbitrary code via the component "/src/main/java/com/dotmarketing/filters/CMSFilter.java".	9.8	More Details
CVE-2021-38408	A stack-based buffer overflow vulnerability in Advantech WebAccess Versions 9.02 and prior caused by a lack of proper validation of the length of user-supplied data may allow remote code execution.	9.8	More Details
CVE-2021-28494	In Arista's MOS (Metamako Operating System) software which is supported on the 7130 product line, under certain conditions, authentication is bypassed by unprivileged users who are accessing the Web UI. This issue affects: Arista Metamako Operating System MOS-0.34.0 and prior releases	9.6	More Details
CVE-2021-23037	On all versions of 16.1.x, 16.0.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	9.6	More Details
CVE-2021-28813	A vulnerability involving insecure storage of sensitive information has been reported to affect QSW-M2116P-2T2S and QNAP switches running QuNetSwitch. If exploited, this vulnerability allows remote attackers to read sensitive information by accessing the unrestricted storage mechanism.We have already fixed this vulnerability in the following versions: QSW-M2116P-2T2S 1.0.6 build 210713 and later QGD-1600P: QuNetSwitch 1.0.6.1509 and later QGD-1602P: QuNetSwitch 1.0.6.1509 and later QGD-3014PT: QuNetSwitch 1.0.6.1519 and later	9.6	More Details
CVE-2021-33672	Due to missing encoding in SAP Contact Center's Communication Desktop component- version 700, an attacker could send malicious script in chat message. When the message is accepted by the chat recipient, the script gets executed in their scope. Due to the usage of ActiveX in the application, the attacker can further execute operating system level commands in the chat recipient's scope. This could lead to a complete compromise of their confidentiality, integrity, and could temporarily impact their availability.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11264	Improper authentication of Non-EAPOL/WAPI plaintext frames during four-way handshake can lead to arbitrary network packet injection in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	9.1	More Details
CVE-2020-11301	Improper authentication of un-encrypted plaintext Wi-Fi frames in an encrypted network can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.1	More Details
CVE-2021-38555	An XML external entity (XXE) injection vulnerability was discovered in the Any23 StreamUtils.java file and is known to affect Any23 versions < 2.5. XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access.	9.1	More Details
CVE-2021-23038	On version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3.1, 14.1.x before 14.1.4.2, 13.1.x before 13.1.4.1, and all versions of 12.1.x, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	9.0	More Details
CVE-2021-35493	The WebFOCUS Reporting Server and WebFOCUS Client components of TIBCO Software Inc.'s TIBCO WebFOCUS Client, TIBCO WebFOCUS Installer, and TIBCO WebFOCUS Reporting Server contain easily exploitable Stored and Reflected Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker to social engineer a legitimate user with network access to execute scripts targeting the affected system or the victim's local system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO WebFOCUS Client: versions 8207.27.0 and below, TIBCO WebFOCUS Installer: versions 8207.27.0 and below, and TIBCO WebFOCUS Reporting Server: versions 8207.27.0 and below.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-38162	SAP Web Dispatcher versions - 7.49, 7.53, 7.77, 7.81, KRNL64NUC - 7.22, 7.22EXT, 7.49, KRNL64UC -7.22, 7.22EXT, 7.49, 7.53, KERNEL - 7.22, 7.49, 7.53, 7.77, 7.81, 7.83 processes allow an unauthenticated attacker to submit a malicious crafted request over a network to a front-end server which may, over several attempts, result in a back-end server confusing the boundaries of malicious and legitimate messages. This can result in the back-end server executing a malicious payload which can be used to read or modify any information on the server or consume server resources making it temporarily unavailable.	8.9	More Details
CVE-2021-35217	Insecure Deseralization of untrusted data remote code execution vulnerability was discovered in Patch Manager Orion Platform Integration module and reported to us by ZDI. An Authenticated Attacker could exploit it by executing WSAsyncExecuteTasks deserialization of untrusted data.	8.9	More Details
CVE-2021-1851	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. An application may be able to execute arbitrary code with kernel privileges.	8.8	More Details
CVE-2021-24727	The StopBadBots WordPress plugin before 6.60 did not validate or escape the order and orderby GET parameter in some of its admin dashboard pages, leading to Authenticated SQL Injections	8.8	More Details
CVE-2021-24728	The Membership & Content Restriction – Paid Member Subscriptions WordPress plugin before 2.4.2 did not sanitise, validate or escape its order and orderby parameters before using them in SQL statement, leading to Authenticated SQL Injections in the Members and Payments pages.	8.8	More Details
CVE-2021-1817	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-20670	An arbitrary file upload vulnerability in /admin/media/upload of ZKEACMS V3.2.0 allows attackers to execute arbitrary code via a crafted HTML file.	8.8	More Details
CVE-2020-20671	A cross-site request forgery (CSRF) in KiteCMS V1.1 allows attackers to arbitrarily add an administrator account.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30802	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 14.7, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-30800	This issue was addressed with improved checks. This issue is fixed in iOS 14.7. Joining a malicious Wi-Fi network may result in a denial of service or arbitrary code execution.	8.8	More Details
CVE-2021-30799	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-30797	This issue was addressed with improved checks. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to code execution.	8.8	More Details
CVE-2021-30795	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-37173	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.14.1), RUGGEDCOM ROX RX1400 (All versions < V2.14.1), RUGGEDCOM ROX RX1500 (All versions < V2.14.1), RUGGEDCOM ROX RX1501 (All versions < V2.14.1), RUGGEDCOM ROX RX1510 (All versions < V2.14.1), RUGGEDCOM ROX RX1511 (All versions < V2.14.1), RUGGEDCOM ROX RX1512 (All versions < V2.14.1), RUGGEDCOM ROX RX1524 (All versions < V2.14.1), RUGGEDCOM ROX RX1536 (All versions < V2.14.1), RUGGEDCOM ROX RX5000 (All versions < V2.14.1). The command line interface of affected devices insufficiently restrict file read and write operations for low privileged users. This could allow an authenticated remote attacker to escalate privileges and gain root access to the device.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37174	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.14.1), RUGGEDCOM ROX RX1400 (All versions < V2.14.1), RUGGEDCOM ROX RX1500 (All versions < V2.14.1), RUGGEDCOM ROX RX1501 (All versions < V2.14.1), RUGGEDCOM ROX RX1510 (All versions < V2.14.1), RUGGEDCOM ROX RX1511 (All versions < V2.14.1), RUGGEDCOM ROX RX1512 (All versions < V2.14.1), RUGGEDCOM ROX RX1524 (All versions < V2.14.1), RUGGEDCOM ROX RX1536 (All versions < V2.14.1), RUGGEDCOM ROX RX5000 (All versions < V2.14.1). The affected devices have a privilege escalation vulnerability, if exploited, an attacker could gain root user access.	8.8	More Details
CVE-2021-37201	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP1). The web interface of affected devices is vulnerable to a Cross-Site Request Forgery (CSRF) attack. This could allow an attacker to manipulate the SINEC NMS configuration by tricking an unsuspecting user with administrative privileges to click on a malicious link.	8.8	More Details
CVE-2021-30762	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.5.4. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited..	8.8	More Details
CVE-2021-30761	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.5.4. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited..	8.8	More Details
CVE-2021-30758	A type confusion issue was addressed with improved state handling. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-40355	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.8), Teamcenter V13.0 (All versions < V13.0.0.7), Teamcenter V13.1 (All versions < V13.1.0.5), Teamcenter V13.2 (All versions < 13.2.0.2). The affected application contains Insecure Direct Object Reference (IDOR) vulnerability that allows an attacker to use user-supplied input to access objects directly.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37531	SAP NetWeaver Knowledge Management XML Forms versions - 7.10, 7.11, 7.30, 7.31, 7.40, 7.50, contains an XSLT vulnerability which allows a non-administrative authenticated attacker to craft a malicious XSL stylesheet file containing a script with OS-level commands, copy it into a location to be accessed by the system and then create a file which will trigger the XSLT engine to execute the script contained within the malicious XSL file. This can result in a full compromise of the confidentiality, integrity, and availability of the system.	8.8	More Details
CVE-2021-24620	The WordPress Simple Ecommerce Shopping Cart Plugin- Sell products through Paypal plugin through 2.2.5 does not check for the uploaded Downloadable Digital product file, allowing any file, such as PHP to be uploaded by an administrator. Furthermore, as there is no CSRF in place, attackers could also make a logged admin upload a malicious PHP file, which would lead to RCE	8.8	More Details
CVE-2021-23029	On version 16.0.x before 16.0.1.2, insufficient permission checks may allow authenticated users with guest privileges to perform Server-Side Request Forgery (SSRF) attacks through F5 Advanced Web Application Firewall (WAF) and the BIG-IP ASM Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.8	More Details
CVE-2021-38176	Due to improper input sanitization, an authenticated user with certain specific privileges can remotely call NZDT function modules listed in Solution Section to execute manipulated query or inject ABAP code to gain access to Backend Database. On successful exploitation the threat actor could completely compromise confidentiality, integrity, and availability of the system.	8.8	More Details
CVE-2021-1867	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5, macOS Big Sur 11.3. A malicious application may be able to execute arbitrary code with kernel privileges.	8.8	More Details
CVE-2021-38388	Central Dogma allows privilege escalation with mirroring to the internal dogma repository that has a file managing the authorization of the project.	8.8	More Details
CVE-2021-21105	Adobe Illustrator version 25.2 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote 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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21104	Adobe Illustrator version 25.2 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to remote 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.	8.8	More Details
CVE-2021-21897	A code execution vulnerability exists in the DL_Dxf::handleLWPolylineData functionality of Ribbonsoft dxflib 3.17.0. A specially-crafted .dxf file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-30707	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted audio file may lead to arbitrary code execution.	8.8	More Details
CVE-2020-7873	Download of code without integrity check vulnerability in ActiveX control of Younglimwon Co., Ltd allows the attacker to cause a arbitrary file download and execution.	8.8	More Details
CVE-2020-7874	Download of code without integrity check vulnerability in NEXACRO14 Runtime ActiveX control of tobesoft Co., Ltd allows the attacker to cause an arbitrary file download and execution. This vulnerability is due to incomplete validation of file download URL or file extension.	8.8	More Details
CVE-2021-26608	An arbitrary file download and execution vulnerability was found in the HShell.dll of handysoft Co., Ltd groupware ActiveX module. This issue is due to missing support for integrity check of download URL or downloaded file hash.	8.8	More Details
CVE-2021-30688	A malicious application may be able to break out of its sandbox. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina. A path handling issue was addressed with improved validation.	8.8	More Details
CVE-2021-38723	FUEL CMS 1.5.0 allows SQL Injection via parameter 'col' in /fuel/index.php/fuel/pages/items	8.8	More Details
CVE-2021-30677	This issue was addressed with improved environment sanitization. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave, macOS Big Sur 11.4, watchOS 7.5. A malicious application may be able to break out of its sandbox.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19263	A cross-site request forgery (CSRF) in MipCMS v5.0.1 allows attackers to arbitrarily escalate user privileges to administrator via index.php?s=/user/ApiAdminUser/itemEdit.	8.8	More Details
CVE-2021-30666	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 12.5.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited..	8.8	More Details
CVE-2021-30665	A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 7.4.1, iOS 14.5.1 and iPadOS 14.5.1, tvOS 14.6, iOS 12.5.3, macOS Big Sur 11.3.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited..	8.8	More Details
CVE-2021-30663	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 14.5.1 and iPadOS 14.5.1, tvOS 14.6, iOS 12.5.3, Safari 14.1.1, macOS Big Sur 11.3.1. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-30661	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 14.1, iOS 12.5.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited..	8.8	More Details
CVE-2020-19280	Jeesns 1.4.2 contains a cross-site request forgery (CSRF) which allows attackers to escalate privileges and perform sensitive program operations.	8.8	More Details
CVE-2021-1876	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-1874	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.5 and iPadOS 14.5. An application may be able to execute arbitrary code with kernel privileges.	8.8	More Details
CVE-2021-24491	The Fileviewer WordPress plugin through 2.2 does not have CSRF checks in place when performing actions such as upload and delete files. As a result, attackers could make a logged in administrator delete and upload arbitrary files via a CSRF attack	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24726	The WP Simple Booking Calendar WordPress plugin before 2.0.6 did not escape, validate or sanitise the orderby parameter in its Search Calendars action, before using it in a SQL statement, leading to an authenticated SQL injection issue	8.8	More Details
CVE-2021-30749	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-23025	On version 15.1.x before 15.1.0.5, 14.1.x before 14.1.3.1, 13.1.x before 13.1.3.5, and all versions of 12.1.x and 11.6.x, an authenticated remote command execution vulnerability exists in the BIG-IP Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.8	More Details
CVE-2021-30734	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-23040	On BIG-IP AFM version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3, 14.1.x before 14.1.4.2, 13.1.x before 13.1.4.1, and all versions of 12.1.x, a SQL injection vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. This issue is exposed only when BIG-IP AFM is provisioned. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.8	More Details
CVE-2021-23026	BIG-IP version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3, 14.1.x before 14.1.4.2, 13.1.x before 13.1.4.1, and all versions of 12.1.x and 11.6.x and all versions of BIG-IQ 8.x, 7.x, and 6.x are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.8	More Details
CVE-2021-36182	A Improper neutralization of special elements used in a command ('Command Injection') in Fortinet FortiWeb version 6.3.13 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests	8.8	More Details
CVE-2021-30737	A memory corruption issue in the ASN.1 decoder was addressed by removing the vulnerable code. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, iOS 12.5.4, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted certificate may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28580	Medium by Adobe version 2.4.5.331 (and earlier) is affected by a buffer overflow vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote 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.	8.8	More Details
CVE-2021-28498	In Arista's MOS (Metamako Operating System) software which is supported on the 7130 product line, user enable passwords set in clear text could result in unprivileged users getting complete access to the systems. This issue affects: Arista Metamako Operating System MOS-0.13 and post releases in the MOS-0.1x train MOS-0.26.6 and prior releases in the MOS-0.2x train MOS-0.31.1 and prior releases in the MOS-0.3x train	8.7	More Details
CVE-2021-32833	Emby Server is a personal media server with apps on many devices. In Emby Server on Windows there is a set of arbitrary file read vulnerabilities. This vulnerability is known to exist in version 4.6.4.0 and may not be patched in later versions. Known vulnerable routes are /Videos/Id/hls/PlaylistId/SegmentId.SegmentContainer, /Images/Ratings/theme/name and /Images/MediaInfo/theme/name. For more details including proof of concept code, refer to the referenced GHSL-2021-051. This issue may lead to unauthorized access to the system especially when Emby Server is configured to be accessible from the Internet.	8.6	More Details
CVE-2021-34720	A vulnerability in the IP Service Level Agreements (IP SLA) responder and Two-Way Active Measurement Protocol (TWAMP) features of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause device packet memory to become exhausted or cause the IP SLA process to crash, resulting in a denial of service (DoS) condition. This vulnerability exists because socket creation failures are mishandled during the IP SLA and TWAMP processes. An attacker could exploit this vulnerability by sending specific IP SLA or TWAMP packets to an affected device. A successful exploit could allow the attacker to exhaust the packet memory, which will impact other processes, such as routing protocols, or crash the IP SLA process.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39206	Pomerium is an open source identity-aware access proxy. Envoy, which Pomerium is based on, contains two authorization related vulnerabilities CVE-2021-32777 and CVE-2021-32779. This may lead to incorrect routing or authorization policy decisions. With specially crafted requests, incorrect authorization or routing decisions may be made by Pomerium. Pomerium v0.14.8 and v0.15.1 contain an upgraded envoy binary with these vulnerabilities patched. This issue can only be triggered when using path prefix based policy. Removing any such policies should provide mitigation.	8.6	More Details
CVE-2021-26603	A heap overflow issue was found in ARK library of bandisoft Co., Ltd when the Ark_DigPathA function parsed a file path. This vulnerability is due to missing support for string length check.	8.6	More Details
CVE-2021-39162	Pomerium is an open source identity-aware access proxy. Envoy, which Pomerium is based on, can abnormally terminate if an H/2 GOAWAY and SETTINGS frame are received in the same IO event. This can lead to a DoS in the presence of untrusted *upstream* servers. 0.15.1 contains an upgraded envoy binary with this vulnerability patched. If only trusted upstreams are configured, there is not substantial risk of this condition being triggered.	8.6	More Details
CVE-2021-39207	parlai is a framework for training and evaluating AI models on a variety of openly available dialogue datasets. In affected versions the package is vulnerable to YAML deserialization attack caused by unsafe loading which leads to Arbitary code execution. This security bug is patched by avoiding unsafe loader users should update to version above v1.1.0. If upgrading is not possible then users can change the Loader used to SafeLoader as a workaround. See commit 507d066ef432ea27d3e201da08009872a2f37725 for details.	8.4	More Details
CVE-2021-28493	In Arista's MOS (Metamako Operating System) software which is supported on the 7130 product line, under certain conditions, a user may be able to execute commands despite not having the privileges to do so. This issue affects: Arista Metamako Operating System All releases in the MOS-0.1x train MOS-0.32.0 and prior releases	8.4	More Details
CVE-2021-30294	Potential null pointer dereference in KGSL GPU auxiliary command due to improper validation of user input in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2021-30290	Possible null pointer dereference due to race condition between timeline fence signal and time line fence destroy in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1934	Possible memory corruption due to improper check when application loader object is explicitly destructed while application is unloading in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT	8.4	More Details
CVE-2021-30295	Possible heap overflow due to improper validation of local variable while storing current task information locally in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	8.4	More Details
CVE-2021-38360	The wp-publications WordPress plugin is vulnerable to restrictive local file inclusion via the Q_FILE parameter found in the ~/bibtexbrowser.php file which allows attackers to include local zip files and achieve remote code execution, in versions up to and including 0.0.	8.3	More Details
CVE-2021-28571	Adobe After Effects version 18.1 (and earlier) is affected by a potential Command injection vulnerability when chained with a development and debugging tool for JavaScript scripts. 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.	8.3	More Details
CVE-2021-32834	Eclipse Keti is a service that was designed to protect RESTfuls API using Attribute Based Access Control (ABAC). In Keti a user able to create Policy Sets can run arbitrary code by sending malicious Groovy scripts which will escape the configured Groovy sandbox. This vulnerability is known to exist in the latest commit at the time of writing this CVE (commit a1c8dbe). For more details see the referenced GHSL-2021-063.	8.2	More Details
CVE-2021-38324	The SP Rental Manager WordPress plugin is vulnerable to SQL Injection via the orderby parameter found in the ~/user/shortcodes.php file which allows attackers to retrieve information contained in a site's database, in versions up to and including 1.5.3.	8.2	More Details
CVE-2021-41033	In all released versions of Eclipse Equinox, at least until version 4.21 (September 2021), installation can be vulnerable to man-in-the-middle attack if using p2 repos that are HTTP; that can then be exploited to serve incorrect p2 metadata and entirely alter the local installation, particularly by installing plug-ins that may then run malicious code.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41072	squashfs_opendir in unsquash-2.c in Squashfs-Tools 4.5 allows Directory Traversal, a different vulnerability than CVE-2021-40153. A squashfs filesystem that has been crafted to include a symbolic link and then contents under the same filename in a filesystem can cause unsquashfs to first create the symbolic link pointing outside the expected directory, and then the subsequent write operation will cause the unsquashfs process to write through the symbolic link elsewhere in the filesystem.	8.1	More Details
CVE-2021-3051	An improper verification of cryptographic signature vulnerability exists in Cortex XSOAR SAML authentication that enables an unauthenticated network-based attacker with specific knowledge of the Cortex XSOAR instance to access protected resources and perform unauthorized actions on the Cortex XSOAR server. This issue impacts: Cortex XSOAR 5.5.0 builds earlier than 1578677; Cortex XSOAR 6.0.2 builds earlier than 1576452; Cortex XSOAR 6.1.0 builds earlier than 1578663; Cortex XSOAR 6.2.0 builds earlier than 1578666. All Cortex XSOAR instances hosted by Palo Alto Networks are protected from this vulnerability; no additional action is required for these instances.	8.1	More Details
CVE-2021-30717	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. An attacker in a privileged network position may be able to execute arbitrary code.	8.1	More Details
CVE-2021-34718	A vulnerability in the SSH Server process of Cisco IOS XR Software could allow an authenticated, remote attacker to overwrite and read arbitrary files on the local device. This vulnerability is due to insufficient input validation of arguments that are supplied by the user for a specific file transfer method. An attacker with lower-level privileges could exploit this vulnerability by specifying Secure Copy Protocol (SCP) parameters when authenticating to a device. A successful exploit could allow the attacker to elevate their privileges and retrieve and upload files on a device that they should not have access to.	8.1	More Details
CVE-2021-3052	A reflected cross-site scripting (XSS) vulnerability in the Palo Alto Network PAN-OS web interface enables an authenticated network-based attacker to mislead another authenticated PAN-OS administrator to click on a specially crafted link that performs arbitrary actions in the PAN-OS web interface as the targeted authenticated administrator. This issue impacts: PAN-OS 8.1 versions earlier than 8.1.20; PAN-OS 9.0 versions earlier than 9.0.14; PAN-OS 9.1 versions earlier than 9.1.10; PAN-OS 10.0 versions earlier than 10.0.2. This issue does not affect Prisma Access.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36179	A stack-based buffer overflow in Fortinet FortiWeb version 6.3.14 and below, 6.2.4 and below allows attacker to execute unauthorized code or commands via crafted parameters in CLI command execution	8.0	More Details
CVE-2021-22528	Reflected Cross Site Scripting (XSS) vulnerability in NetIQ Access Manager prior to 5.0.1 and 4.5.4	8.0	More Details
CVE-2021-1853	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.3. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2021-30605	Inappropriate implementation in the ChromeOS Readiness Tool installer on Windows prior to 1.0.2.0 loosens DCOM access rights on two objects allowing an attacker to potentially bypass discretionary access controls.	7.8	More Details
CVE-2021-30764	Processing a maliciously crafted file may lead to arbitrary code execution. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. This issue was addressed with improved checks.	7.8	More Details
CVE-2021-30765	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-40867	Certain NETGEAR smart switches are affected by an authentication hijacking race-condition vulnerability by an unauthenticated attacker who uses the same source IP address as an admin in the process of logging in (e.g., behind the same NAT device, or already in possession of a foothold on an admin's machine). This occurs because the multi-step HTTP authentication process is effectively tied only to the source IP address. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	7.8	More Details
CVE-2021-30701	This issue was addressed with improved checks. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1858	Processing a maliciously crafted image may lead to arbitrary code execution. This issue is fixed in Security Update 2021-002 Catalina, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. An out-of-bounds write issue was addressed with improved bounds checking.	7.8	More Details
CVE-2021-32136	Heap buffer overflow in the print_udta function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file.	7.8	More Details
CVE-2021-30766	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-30781	This issue was addressed with improved checks. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-005 Mojave, Security Update 2021-004 Catalina. A local attacker may be able to cause unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-30703	A double free issue was addressed with improved memory management. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave, macOS Big Sur 11.4, watchOS 7.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-30742	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 14.5 and iPadOS 14.5. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30724	This issue was addressed with improved checks. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2021-30704	A logic issue was addressed with improved state management. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-30725	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1847	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-1843	This issue was addressed with improved checks. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-36216	LINE for Windows 6.2.1.2289 and before allows arbitrary code execution via malicious DLL injection.	7.8	More Details
CVE-2021-1840	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2021-1839	The issue was addressed with improved permissions logic. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2021-1868	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2021-30693	A validation issue was addressed with improved logic. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30726	A malicious application may be able to execute arbitrary code with kernel privileges. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. An out-of-bounds write issue was addressed with improved bounds checking.	7.8	More Details
CVE-2021-1875	A double free issue was addressed with improved memory management. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. Processing a maliciously crafted file may lead to heap corruption.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30675	A memory corruption issue was addressed with improved state management. This issue is fixed in Boot Camp 6.1.14. A malicious application may be able to elevate privileges.	7.8	More Details
CVE-2021-30679	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2021-30748	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 14.7, macOS Big Sur 11.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-30680	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4. A local user may be able to load unsigned kernel extensions.	7.8	More Details
CVE-2021-30681	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2021-30664	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. Processing a maliciously crafted file may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30683	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A malicious application could execute arbitrary code leading to compromise of user information.	7.8	More Details
CVE-2021-30684	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina. A remote attacker may cause an unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-34719	Multiple vulnerabilities in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker with a low-privileged account to elevate privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1923	Incorrect pointer argument passed to trusted application TA could result in un-intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	7.8	More Details
CVE-2021-30653	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-28701	Another race in XENMAPSPACE_grant_table handling Guests are permitted access to certain Xen-owned pages of memory. The majority of such pages remain allocated / associated with a guest for its entire lifetime. Grant table v2 status pages, however, are de-allocated when a guest switches (back) from v2 to v1. Freeing such pages requires that the hypervisor enforce that no parallel request can result in the addition of a mapping of such a page to a guest. That enforcement was missing, allowing guests to retain access to pages that were freed and perhaps re-used for other purposes. Unfortunately, when XSA-379 was being prepared, this similar issue was not noticed.	7.8	More Details
CVE-2021-1885	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30759	A stack overflow was addressed with improved input validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-005 Mojave, Security Update 2021-004 Catalina. Processing a maliciously crafted font file may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30760	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-005 Mojave, Security Update 2021-004 Catalina. Processing a maliciously crafted font file may lead to arbitrary code execution.	7.8	More Details
CVE-2021-1881	An out-of-bounds read was addressed with improved input validation. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. Processing a maliciously crafted font file may lead to arbitrary code execution.	7.8	More Details
CVE-2021-1880	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.3, watchOS 7.4. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30743	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, Security Update 2021-003 Catalina, tvOS 14.5, macOS Big Sur 11.3. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30752	Processing a maliciously crafted image may lead to arbitrary code execution. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. An out-of-bounds read was addressed with improved input validation.	7.8	More Details
CVE-2021-1838	This issue was addressed with improved checks. This issue is fixed in iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-1841	A malicious application may be able to execute arbitrary code with kernel privileges. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina. An out-of-bounds write issue was addressed with improved bounds checking.	7.8	More Details
CVE-2021-30672	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2021-30740	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-30774	A logic issue was addressed with improved validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2021-30790	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-1762	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.4 and iPadOS 14.4, macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30775	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-004 Catalina. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30708	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2020-27942	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave. Processing a maliciously crafted font file may lead to arbitrary code execution.	7.8	More Details
CVE-2021-25665	A vulnerability has been identified in Simcenter STAR-CCM+ Viewer (All versions < V2021.2.1). The starview+.exe application lacks proper validation of user-supplied data when parsing scene files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13700)	7.8	More Details
CVE-2020-20672	An arbitrary file upload vulnerability in /admin/upload/uploadfile of KiteCMS V1.1 allows attackers to getshell via a crafted PHP file.	7.8	More Details
CVE-2021-33362	Stack buffer overflow in the hevc_parse_vps_extension function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file.	7.8	More Details
CVE-2021-30777	An injection issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2021-30739	A local attacker may be able to elevate their privileges. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A memory corruption issue was addressed with improved validation.	7.8	More Details
CVE-2021-30735	A malicious application may be able to execute arbitrary code with kernel privileges. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. An out-of-bounds write issue was addressed with improved bounds checking.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30792	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30736	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-30779	This issue was addressed with improved checks. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30780	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-005 Mojave, Security Update 2021-004 Catalina. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2021-1952	Possible buffer over read occurs due to lack of length check of request buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	7.8	More Details
CVE-2021-30789	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-004 Catalina. Processing a maliciously crafted font file may lead to arbitrary code execution.	7.8	More Details
CVE-2021-30784	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.5. A local attacker may be able to execute code on the Apple T2 Security Chip.	7.8	More Details
CVE-2021-1833	This issue was addressed with improved checks. This issue is fixed in iOS 14.5 and iPadOS 14.5. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2021-30787	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. An application may be able to cause unexpected system termination or write kernel memory.	7.8	More Details
CVE-2021-1812	A logic issue was addressed with improved validation. This issue is fixed in iOS 14.5 and iPadOS 14.5. A malicious application may be able to execute arbitrary code with system privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1813	A validation issue was addressed with improved logic. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2021-37202	A vulnerability has been identified in NX 1980 Series (All versions < V1984), Solid Edge SE2021 (All versions < SE2021MP8). The IFC adapter in affected application contains a use-after-free vulnerability that could be triggered while parsing user-supplied IFC files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-1814	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.3, watchOS 7.4. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-34728	Multiple vulnerabilities in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker with a low-privileged account to elevate privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	7.8	More Details
CVE-2021-1816	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-30728	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-30712	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-30713	A permissions issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.4. A malicious application may be able to bypass Privacy preferences. Apple is aware of a report that this issue may have been actively exploited..	7.8	More Details
CVE-2021-30785	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-004 Catalina. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30772	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.5. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2021-37200	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP1). An attacker with access to the webserver of an affected system could download arbitrary files from the underlying filesystem by sending a specially crafted HTTP request.	7.7	More Details
CVE-2021-28816	A stack buffer overflow vulnerability has been reported to affect QNAP device running QTS, QuTScloud, QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QTS, QuTScloud, QuTS hero: QTS 4.5.4.1715 build 20210630 and later QTS 5.0.0.1716 build 20210701 and later QTS 4.3.3.1693 build 20210624 and later QTS 4.3.6.1750 build 20210730 and later QuTScloud c4.5.6.1755 and later QuTS hero h4.5.4.1771 build 20210825 and later	7.6	More Details
CVE-2021-39201	WordPress is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database. ### Impact The issue allows an authenticated but low-privileged user (like contributor/author) to execute XSS in the editor. This bypasses the restrictions imposed on users who do not have the permission to post `unfiltered_html`. ### Patches This has been patched in WordPress 5.8, and will be pushed to older versions via minor releases (automatic updates). It's strongly recommended that you keep auto-updates enabled to receive the fix. ### References https://wordpress.org/news/category/releases/ https://hackerone.com/reports/1142140 ### For more information If you have any questions or comments about this advisory: * Open an issue in [HackerOne](https://hackerone.com/wordpress)	7.6	More Details
CVE-2021-23435	This affects the package clearance before 2.5.0. The vulnerability can be possible when users are able to set the value of session[:return_to]. If the value used for return_to contains multiple leading slashes (/////example.com) the user ends up being redirected to the external domain that comes after the slashes (http://example.com).	7.6	More Details
CVE-2021-23404	This affects all versions of package sqlite-web. The SQL dashboard area allows sensitive actions to be performed without validating that the request originated from the application. This could enable an attacker to trick a user into performing these actions unknowingly through a Cross Site Request Forgery (CSRF) attack.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39202	WordPress is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database. In affected versions the widgets editor introduced in WordPress 5.8 beta 1 has improper handling of HTML input in the Custom HTML feature. This leads to stored XSS in the custom HTML widget. This has been patched in WordPress 5.8. It was only present during the testing/beta phase of WordPress 5.8.	7.6	More Details
CVE-2021-23039	On version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3, 14.1.x before 14.1.2.8, and all versions of 13.1.x and 12.1.x, when IPSec is configured on a BIG-IP system, undisclosed requests from an authorized remote (IPSec) peer, which already has a negotiated Security Association, can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-3053	An improper handling of exceptional conditions vulnerability exists in the Palo Alto Networks PAN-OS dataplane that enables an unauthenticated network-based attacker to send specifically crafted traffic through the firewall that causes the service to crash. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.1.9; PAN-OS 10.0 versions earlier than PAN-OS 10.0.5. This issue does not affect Prisma Access.	7.5	More Details
CVE-2021-32485	In modem 2G RRM, there is a possible system crash due to a heap buffer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00500621; Issue ID: ALPS04964926.	7.5	More Details
CVE-2021-40346	An integer overflow exists in HAProxy 2.0 through 2.5 in htx_add_header that can be exploited to perform an HTTP request smuggling attack, allowing an attacker to bypass all configured http-request HAProxy ACLs and possibly other ACLs.	7.5	More Details
CVE-2020-19137	Incorrect Access Control in Autumn v1.0.4 and earlier allows remote attackers to obtain clear-text login credentials via the component "autumn-cms/user/getAllUser/?page=1&limit=10".	7.5	More Details
CVE-2021-32484	In modem 2G RRM, there is a possible system crash due to a heap buffer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00500621; Issue ID: ALPS04964917.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3761	Any CA issuer in the RPKI can trick OctoRPKI prior to 1.3.0 into emitting an invalid VRP "MaxLength" value, causing RTR sessions to terminate. An attacker can use this to disable RPKI Origin Validation in a victim network (for example AS 13335 - Cloudflare) prior to launching a BGP hijack which during normal operations would be rejected as "RPKI invalid". Additionally, in certain deployments RTR session flapping in and of itself also could cause BGP routing churn, causing availability issues.	7.5	More Details
CVE-2021-1914	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2021-33982	An insufficient session expiration vulnerability exists in the "Fish I Hunt FL" iOS app version 3.8.0 and earlier, which allows a remote attacker to reuse, spoof, or steal other user and admin sessions.	7.5	More Details
CVE-2021-23036	On version 16.0.x before 16.0.1.2, when a BIG-IP ASM and DataSafe profile are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-1948	Possible out of bound read due to lack of length check of data while parsing the beacon or probe response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-23030	On BIG-IP Advanced WAF and BIG-IP ASM version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3.1, 14.1.x before 14.1.4.3, 13.1.x before 13.1.4.1, and all versions of 12.1.x, when a WebSocket profile is configured on a virtual server, undisclosed requests can cause bd to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-30698	A null pointer dereference was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.4, Safari 14.1.1, iOS 14.6 and iPadOS 14.6. A remote attacker may be able to cause a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23028	On version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3.1, 14.1.x before 14.1.4.2, and 13.1.x before 13.1.4, when JSON content profiles are configured for URLs as part of an F5 Advanced Web Application Firewall (WAF)/BIG-IP ASM security policy and applied to a virtual server, undisclosed requests may cause the BIG-IP ASM bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-1971	Possible assertion due to lack of physical layer state validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-1974	Possible buffer over read due to lack of alignment between map or unmap length of IPA SMMU and WLAN SMMU in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-32486	In modem 2G RRM, there is a possible system crash due to a heap buffer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00500621; Issue ID: ALPS04964928.	7.5	More Details
CVE-2021-30715	A logic issue was addressed with improved state management. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted message may lead to a denial of service.	7.5	More Details
CVE-2021-1941	Possible buffer over read issue due to improper length check on WPA IE string sent by peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-23045	On BIG-IP version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3.1, 14.1.x before 14.1.4.3, 13.1.x before 13.1.4.1, and all versions of 12.1.x, when an SCTP profile with multiple paths is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32487	In modem 2G RRM, there is a possible system crash due to a heap buffer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00500736; Issue ID: ALPS04938456.	7.5	More Details
CVE-2021-23050	On BIG-IP Advanced WAF and BIG-IP ASM version 16.0.x before 16.0.1.2 and 15.1.x before 15.1.3 and NGINX App Protect on all versions before 3.5.0, when a cross-site request forgery (CSRF)-enabled policy is configured on a virtual server, an undisclosed HTML response may cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-1849	An issue in code signature validation was addressed with improved checks. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. A malicious application may be able to bypass Privacy preferences.	7.5	More Details
CVE-2021-23035	On BIG-IP 14.1.x before 14.1.4.4, when an HTTP profile is configured on a virtual server, after a specific sequence of packets, chunked responses can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-1809	A memory corruption issue was addressed with improved validation. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. A malicious application may be able to read restricted memory.	7.5	More Details
CVE-2021-1808	A memory corruption issue was addressed with improved validation. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. An application may be able to read restricted memory.	7.5	More Details
CVE-2021-1784	A permissions issue existed in DiskArbitration. This was addressed with additional ownership checks. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave. A malicious application may be able to modify protected parts of the file system.	7.5	More Details
CVE-2021-41054	tftpd_file.c in atftp through 0.7.4 has a buffer overflow because buffer-size handling does not properly consider the combination of data, OACK, and other options.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30729	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 14.6 and iPadOS 14.6. A device may accept invalid activation results.	7.5	More Details
CVE-2021-23051	On BIG-IP versions 15.1.0.4 through 15.1.3, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP on Amazon Web Services (AWS) systems, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. This is due to an incomplete fix for CVE-2020-5862. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-30798	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6. A malicious application may be able to bypass certain Privacy preferences.	7.5	More Details
CVE-2021-1859	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.3. Locked Notes content may have been unexpectedly unlocked.	7.5	More Details
CVE-2021-39123	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability in the /rest/gadget/1.0/createdVsResolved/generate endpoint. The affected versions are before version 8.16.0.	7.5	More Details
CVE-2021-23049	On BIG-IP version 16.0.x before 16.0.1.2 and 15.1.x before 15.1.3, when the iRules RESOLVER::summarize command is used on a virtual server, undisclosed requests can cause an increase in Traffic Management Microkernel (TMM) memory utilization resulting in an out-of-memory condition and a denial-of-service (DoS). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-33720	A vulnerability has been identified in SIPROTEC 5 relays with CPU variants CP050 (All versions < V8.80), SIPROTEC 5 relays with CPU variants CP100 (All versions < V8.80), SIPROTEC 5 relays with CPU variants CP300 (All versions < V8.80). Specially crafted packets sent to port 4443/tcp could cause a Denial-of-Service condition.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33737	A vulnerability has been identified in SIMATIC CP 343-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 343-1 Advanced (incl. SIPLUS variants) (All versions), SIMATIC CP 343-1 ERPC (All versions), SIMATIC CP 343-1 Lean (incl. SIPLUS variants) (All versions), SIMATIC CP 443-1 (All versions < V3.3), SIMATIC CP 443-1 (All versions < V3.3), SIMATIC CP 443-1 Advanced (All versions < V3.3), SIPLUS NET CP 443-1 (All versions < V3.3), SIPLUS NET CP 443-1 Advanced (All versions < V3.3). Sending a specially crafted packet to port 102/tcp of an affected device could cause a denial of service condition. A restart is needed to restore normal operations.	7.5	More Details
CVE-2021-37206	A vulnerability has been identified in SIPROTEC 5 relays with CPU variants CP050 (All versions < V8.80), SIPROTEC 5 relays with CPU variants CP100 (All versions < V8.80), SIPROTEC 5 relays with CPU variants CP300 (All versions < V8.80). Received webpackets are not properly processed. An unauthenticated remote attacker with access to any of the Ethernet interfaces could send specially crafted packets to force a restart of the target device.	7.5	More Details
CVE-2021-23048	On BIG-IP version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3.1, 14.1.x before 14.1.4.3, 13.1.x before 13.1.4.1, and all versions of 12.1.x and 11.6.x, when GPRS Tunneling Protocol (GTP) iRules commands or a GTP profile is configured on a virtual server, undisclosed GTP messages can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-38177	SAP CommonCryptoLib version 8.5.38 or lower is vulnerable to null pointer dereference vulnerability when an unauthenticated attacker sends crafted malicious data in the HTTP requests over the network, this causes the SAP application to crash and has high impact on the availability of the SAP system.	7.5	More Details
CVE-2021-40356	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.8), Teamcenter V13.0 (All versions < V13.0.0.7), Teamcenter V13.1 (All versions < V13.1.0.5), Teamcenter V13.2 (All versions < 13.2.0.2). The application contains a XML External Entity Injection (XXE) vulnerability. This could allow an attacker to view files on the application server filesystem.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23042	On BIG-IP version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3, 14.1.x before 14.1.4, 13.1.x before 13.1.4, and 12.1.x before 12.1.6, when an HTTP profile is configured on a virtual server, undisclosed requests can cause a significant increase in system resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-32836	ZStack is open source IaaS(infrastructure as a service) software. In ZStack before versions 3.10.12 and 4.1.6 there is a pre-auth unsafe deserialization vulnerability in the REST API. An attacker in control of the request body will be able to provide both the class name and the data to be deserialized and therefore will be able to instantiate an arbitrary type and assign arbitrary values to its fields. This issue may lead to a Denial Of Service. If a suitable gadget is available, then an attacker may also be able to exploit this vulnerability to gain pre-auth remote code execution. For additional details see the referenced GHSL-2021-087.	7.5	More Details
CVE-2021-41077	The activation process in Travis CI, for certain 2021-09-03 through 2021-09-10 builds, causes secret data to have unexpected sharing that is not specified by the customer-controlled .travis.yml file. In particular, the desired behavior (if .travis.yml has been created locally by a customer, and added to git) is for a Travis service to perform builds in a way that prevents public access to customer-specific secret environment data such as signing keys, access credentials, and API tokens. However, during the stated 8-day interval, secret data could be revealed to an unauthorized actor who forked a public repository and printed files during a build process.	7.5	More Details
CVE-2021-23032	On version 16.x before 16.1.0, 15.1.x before 15.1.3.1, 14.1.x before 14.1.4.4, and all versions of 13.1.x and 12.1.x, when a BIG-IP DNS system is configured with non-default Wide IP and pool settings, undisclosed DNS responses can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-28910	BAB TECHNOLOGIE GmbH eibPort V3 prior version 3.9.1 contains basic SSRF vulnerability. It allow unauthenticated attackers to request to any internal and external server.	7.5	More Details
CVE-2021-40839	The rencode package through 1.0.6 for Python allows an infinite loop in typecode decoding (such as via ;\x2f\x7f), enabling a remote attack that consumes CPU and memory.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21996	An issue was discovered in SaltStack Salt before 3003.3. A user who has control of the source, and source_hash URLs can gain full file system access as root on a salt minion.	7.5	More Details
CVE-2021-23044	On BIG-IP version 16.x before 16.1.0, 15.1.x before 15.1.3.1, 14.1.x before 14.1.4.2, 13.1.x before 13.1.4.1, and all versions of 12.1.x and 11.6.x, when the Intel QuickAssist Technology (QAT) compression driver is used on affected BIG-IP hardware and BIG-IP Virtual Edition (VE) platforms, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-23034	On BIG-IP version 16.x before 16.1.0 and 15.1.x before 15.1.3.1, when a DNS profile using a DNS cache resolver is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-23033	On BIG-IP Advanced WAF and BIG-IP ASM version 16.x before 16.1.0x, 15.1.x before 15.1.3.1, 14.1.x before 14.1.4.3, 13.1.x before 13.1.4.1, and all versions of 12.1.x, when a WebSocket profile is configured on a virtual server, undisclosed requests can cause bd to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-37414	Zoho ManageEngine DesktopCentral before 10.0.709 allows anyone to get a valid user's APIKEY without authentication.	7.5	More Details
CVE-2021-39204	Pomerium is an open source identity-aware access proxy. Envoy, which Pomerium is based on, incorrectly handles resetting of HTTP/2 streams with excessive complexity. This can lead to high CPU utilization when a large number of streams are reset. This can result in a DoS condition. Pomerium versions 0.14.8 and 0.15.1 contain an upgraded envoy binary with this vulnerability patched.	7.5	More Details
CVE-2021-30660	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. A malicious application may be able to disclose kernel memory.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34713	A vulnerability in the Layer 2 punt code of Cisco IOS XR Software running on Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, adjacent attacker to cause the affected line card to reboot. This vulnerability is due to incorrect handling of specific Ethernet frames that cause a spin loop that can make the network processors unresponsive. An attacker could exploit this vulnerability by sending specific types of Ethernet frames on the segment where the affected line cards are attached. A successful exploit could allow the attacker to cause the affected line card to reboot.	7.4	More Details
CVE-2020-27969	Yandex Browser for Android 20.8.4 allows remote attackers to perform SOP bypass and addresss bar spoofing	7.3	More Details
CVE-2021-30662	This issue was addressed with improved checks. This issue is fixed in iOS 14.5 and iPadOS 14.5. Processing a maliciously crafted file may lead to arbitrary code execution.	7.3	More Details
CVE-2021-23440	This affects the package set-value before <2.0.1, >=3.0.0 <4.0.1. A type confusion vulnerability can lead to a bypass of CVE-2019-10747 when the user-provided keys used in the path parameter are arrays.	7.3	More Details
CVE-2021-1909	Buffer overflow occurs in trusted applications due to lack of length check of parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.3	More Details
CVE-2021-3054	A time-of-check to time-of-use (TOCTOU) race condition vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator with permission to upload plugins to execute arbitrary code with root user privileges. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11; PAN-OS 10.0 versions earlier than PAN-OS 10.0.7; PAN-OS 10.1 versions earlier than PAN-OS 10.1.2. This issue does not affect Prisma Access.	7.2	More Details
CVE-2021-33554	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to command injection, which may allow an attacker to remotely execute arbitrary code.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32805	Flask-AppBuilder is an application development framework, built on top of Flask. In affected versions if using Flask-AppBuilder OAuth, an attacker can share a carefully crafted URL with a trusted domain for an application built with Flask-AppBuilder, this URL can redirect a user to a malicious site. This is an open redirect vulnerability. To resolve this issue upgrade to Flask-AppBuilder 3.2.2 or above. If upgrading is infeasible users may filter HTTP traffic containing `?next={next-site}` where the `next-site` domain is different from the application you are protecting as a workaround.	7.2	More Details
CVE-2021-28912	BAB TECHNOLOGIE GmbH eibPort V3. Each device has its own unique hard coded and weak root SSH key passphrase known as 'eibPort string'. This is usable and the final part of an attack chain to gain SSH root access.	7.2	More Details
CVE-2021-28495	In Arista's MOS (Metamako Operating System) software which is supported on the 7130 product line, under certain conditions, user authentication can be bypassed when API access is enabled via the JSON-RPC APIs. This issue affects: Arista Metamako Operating System All releases in the MOS-0.1x train MOS-0.13 and post releases in the MOS-0.1x train MOS-0.26.6 and below releases in the MOS-0.2x train MOS-0.31.1 and below releases in the MOS-0.3x train	7.2	More Details
CVE-2021-40222	Rittal CMC PU III Web management Version affected: V3.11.00_2. Version fixed: V3.17.10 is affected by a remote code execution vulnerablity. It is possible to introduce shell code to create a reverse shell in the PU-Hostname field of the TCP/IP Configuration dialog. Web application fails to sanitize user input on Network TCP/IP configuration page. This allows the attacker to inject commands as root on the device which will be executed once the data is received.	7.2	More Details
CVE-2021-33548	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to command injection, which may allow an attacker to remotely execute arbitrary code.	7.2	More Details
CVE-2021-33545	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to a stack-based buffer overflow condition in the counter parameter which may allow an attacker to remotely execute arbitrary code.	7.2	More Details
CVE-2021-33547	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to a stack-based buffer overflow condition in the profile parameter which may allow an attacker to remotely execute arbitrary code.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33552	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to command injection, which may allow an attacker to remotely execute arbitrary code.	7.2	More Details
CVE-2021-39459	Remote code execution in the modules component in Yakamara Media Redaxo CMS version 5.12.1 allows an authenticated CMS user to execute code on the hosting system via a module containing malicious PHP code.	7.2	More Details
CVE-2021-33551	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to command injection, which may allow an attacker to remotely execute arbitrary code.	7.2	More Details
CVE-2021-33550	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to command injection, which may allow an attacker to remotely execute arbitrary code.	7.2	More Details
CVE-2021-33544	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to command injection, which may allow an attacker to remotely execute arbitrary code.	7.2	More Details
CVE-2021-33549	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to a stack-based buffer overflow condition in the action parameter, which may allow an attacker to remotely execute arbitrary code.	7.2	More Details
CVE-2021-33553	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to command injection, which may allow an attacker to remotely execute arbitrary code.	7.2	More Details
CVE-2021-33546	Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to a stack-based buffer overflow condition in the name parameter, which may allow an attacker to remotely execute arbitrary code.	7.2	More Details
CVE-2021-40354	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.8), Teamcenter V13.0 (All versions < V13.0.0.7), Teamcenter V13.1 (All versions < V13.1.0.5), Teamcenter V13.2 (All versions < 13.2.0.2). The "surrogate" functionality on the user profile of the application does not perform sufficient access control that could lead to an account takeover. Any profile on the application can perform this attack and access any other user assigned tasks via the "inbox/surrogate tasks".	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30788	This issue was addressed with improved checks. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-005 Mojave, Security Update 2021-004 Catalina. Processing a maliciously crafted tiff file may lead to a denial-of-service or potentially disclose memory contents.	7.1	More Details
CVE-2021-30710	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. A malicious application may cause a denial of service or potentially disclose memory contents.	7.1	More Details
CVE-2021-30741	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted mail message may lead to unexpected memory modification or application termination.	7.1	More Details
CVE-2021-37203	A vulnerability has been identified in NX 1980 Series (All versions < V1984), Solid Edge SE2021 (All versions < SE2021MP8). The plmxmlAdapterIFC.dll contains an out-of-bounds read while parsing user supplied IFC files which could result in a read past the end of an allocated buffer. This could allow an attacker to cause a denial-of-service condition or read sensitive information from memory locations.	7.1	More Details
CVE-2021-1828	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave. An application may be able to cause unexpected system termination or write kernel memory.	7.1	More Details
CVE-2021-1935	Possible null pointer dereference due to lack of validation check for passed pointer during key import in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	7.1	More Details
CVE-2021-30719	A local user may be able to cause unexpected system termination or read kernel memory. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina. An out-of-bounds read issue was addressed by removing the vulnerable code.	7.1	More Details
CVE-2021-30676	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A local user may be able to cause unexpected system termination or read kernel memory.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30652	A race condition was addressed with additional validation. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. A malicious application may be able to gain root privileges.	7.0	More Details
CVE-2021-30786	A race condition was addressed with improved state handling. This issue is fixed in iOS 14.7, macOS Big Sur 11.5. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution.	7.0	More Details
CVE-2021-37101	There is an improper authorization vulnerability in AIS-BW50-00 9.0.6.2(H100SP10C00) and 9.0.6.2(H100SP15C00). Due to improper authorization mangement, an attakcer can exploit this vulnerability by physical accessing the device and implant malicious code. Successfully exploit could leads to arbitrary code execution in the target device.	6.8	More Details
CVE-2021-24490	The Email Artillery (MASS EMAIL) WordPress plugin through 4.1 does not properly check the uploaded files from the Import Emails feature, allowing arbitrary files to be uploaded. Furthermore, the plugin is also lacking any CSRF check, allowing such issue to be exploited via a CSRF attack as well. However, due to the presence of a .htaccess, denying access to everything in the folder the file is uploaded to, the malicious uploaded file will only be accessible on Web Servers such as Nginx/IIS	6.8	More Details
CVE-2021-39203	WordPress is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database. In affected versions authenticated users who don't have permission to view private post types/data can bypass restrictions in the block editor under certain conditions. This affected WordPress 5.8 beta during the testing period. It's fixed in the final 5.8 release.	6.8	More Details
CVE-2021-3145	In Ionic Identity Vault before 5, a local root attacker on an Android device can bypass biometric authentication.	6.7	More Details
CVE-2021-1962	Buffer Overflow while processing IOCTL for getting peripheral endpoint information there is no proper validation for input maximum endpoint pair and its size in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	6.7	More Details
CVE-2021-34721	Multiple vulnerabilities in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to gain access to the underlying root shell of an affected device and execute arbitrary commands with root privileges. For more information about these vulnerabilities, see the Details section of this advisory.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20118	Nessus Agent 8.3.0 and earlier was found to contain a local privilege escalation vulnerability which could allow an authenticated, local administrator to run specific executables on the Nessus Agent host. This is different than CVE-2021-20117.	6.7	More Details
CVE-2021-20117	Nessus Agent 8.3.0 and earlier was found to contain a local privilege escalation vulnerability which could allow an authenticated, local administrator to run specific executables on the Nessus Agent host. This is different than CVE-2021-20118.	6.7	More Details
CVE-2021-34722	Multiple vulnerabilities in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to gain access to the underlying root shell of an affected device and execute arbitrary commands with root privileges. For more information about these vulnerabilities, see the Details section of this advisory.	6.7	More Details
CVE-2021-1961	Possible buffer overflow due to lack of offset length check while updating the buffer value in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.7	More Details
CVE-2021-1958	A race condition in fastrpc kernel driver for dynamic process creation can lead to use after free scenario in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables	6.7	More Details
CVE-2021-1963	Possible use-after-free due to lack of validation for the rule count in filter table in IPA driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.7	More Details
CVE-2021-30783	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. A sandboxed process may be able to circumvent sandbox restrictions.	6.5	More Details
CVE-2021-38175	SAP Analysis for Microsoft Office - version 2.8, allows an attacker with high privileges to read sensitive data over the network, and gather or change information in the current system without user interaction. The attack would not lead to an impact on the availability of the system, but there would be an impact on integrity and confidentiality.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40284	D-Link DSL-3782 EU v1.01:EU v1.03 is affected by a buffer overflow which can cause a denial of service. This vulnerability exists in the web interface "/cgi-bin/New_GUI/Igmp.asp". Authenticated remote attackers can trigger this vulnerability by sending a long string in parameter 'igmpsnoopEnable' via an HTTP request.	6.5	More Details
CVE-2021-33685	SAP Business One version - 10.0 allows low-level authorized attacker to traverse the file system to access files or directories that are outside of the restricted directory. A successful attack allows access to high level sensitive data	6.5	More Details
CVE-2021-25466	Improper scheme check vulnerability in Samsung Internet prior to version 15.0.2.47 allows attackers to perform Man-in-the-middle attack and obtain Samsung Account token.	6.5	More Details
CVE-2021-28914	BAB TECHNOLOGIE GmbH eibPort V3 prior version 3.9.1 allow the user to set a weak password because the strength is shown in configuration tool, but finally not enforced. This is usable and part of an attack chain to gain SSH root access.	6.5	More Details
CVE-2021-39458	Triggering an error page of the import process in Yakamara Media Redaxo CMS version 5.12.1 allows an authenticated CMS user has to alternate the files of a vaild file backup. This leads of leaking the database credentials in the environment variables.	6.5	More Details
CVE-2021-30755	Processing a maliciously crafted font may result in the disclosure of process memory. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5. An out-of-bounds read was addressed with improved input validation.	6.5	More Details
CVE-2021-37183	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0 SP2). The affected software allows sending send-to-sleep notifications to the managed devices. An unauthenticated attacker in the same network of the affected system can abuse these notifications to cause a Denial-of-Service condition in the managed devices.	6.5	More Details
CVE-2021-37177	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0 SP2). The status provided by the syslog clients managed by the affected software can be manipulated by an unauthenticated attacker in the same network of the affected system.	6.5	More Details
CVE-2021-25449	An improper input validation vulnerability in libsapeextractor library prior to SMR Sep-2021 Release 1 allows attackers to execute arbitrary code in mediaextractor process.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33716	A vulnerability has been identified in SIMATIC CP 1543-1 (incl. SIPLUS variants) (All versions < V3.0), SIMATIC CP 1545-1 (All versions < V1.1). An attacker with access to the subnet of the affected device could retrieve sensitive information stored in cleartext.	6.5	More Details
CVE-2021-30796	A logic issue was addressed with improved validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. Processing a maliciously crafted image may lead to a denial of service.	6.5	More Details
CVE-2021-1811	A logic issue was addressed with improved state management. This issue is fixed in iTunes 12.11.3 for Windows, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iCloud for Windows 12.3, macOS Big Sur 11.3, watchOS 7.4, tvOS 14.5, iOS 14.5 and iPadOS 14.5. Processing a maliciously crafted font may result in the disclosure of process memory.	6.5	More Details
CVE-2021-1820	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. Processing maliciously crafted web content may result in the disclosure of process memory.	6.5	More Details
CVE-2020-19143	Buffer Overflow in LibTiff v4.0.10 allows attackers to cause a denial of service via the "TIFFVGetField" funtion in the component 'libtiff/tif_dir.c'.	6.5	More Details
CVE-2020-19144	Buffer Overflow in LibTiff v4.0.10 allows attackers to cause a denial of service via the 'in _TIFFmemcpy' funtion in the component 'tif_unix.c'.	6.5	More Details
CVE-2021-30659	A validation issue was addressed with improved logic. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, macOS Big Sur 11.3. A malicious application may be able to leak sensitive user information.	6.5	More Details
CVE-2021-38721	FUEL CMS 1.5.0 login.php contains a cross-site request forgery (CSRF) vulnerability	6.5	More Details
CVE-2020-19264	A cross-site request forgery (CSRF) in MipCMS v5.0.1 allows attackers to arbitrarily add users via index.php?s=/user/ApiAdminUser/itemAdd.	6.5	More Details
CVE-2021-1855	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.3. A malicious website may be able to force unnecessary network connections to fetch its favicon.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1857	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iTunes 12.11.3 for Windows, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iCloud for Windows 12.3, macOS Big Sur 11.3, watchOS 7.4, tvOS 14.5, iOS 14.5 and iPadOS 14.5. Processing maliciously crafted web content may disclose sensitive user information.	6.5	More Details
CVE-2021-1873	An API issue in Accessibility TCC permissions was addressed with improved state management. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave. A malicious application may be able to unexpectedly leak a user's credentials from secure text fields.	6.5	More Details
CVE-2021-38174	When a user opens manipulated files received from untrusted sources in SAP 3D Visual Enterprise Viewer version - 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	6.5	More Details
CVE-2021-38150	When an attacker manages to get access to the local memory, or the memory dump of a victim, for example by a social engineering attack, SAP Business Client versions - 7.0, 7.70, will allow him to read extremely sensitive data, such as credentials. This would allow the attacker to compromise the corresponding backend for which the credentials are valid.	6.5	More Details
CVE-2021-34786	Multiple vulnerabilities in Cisco BroadWorks CommPilot Application Software could allow an authenticated, remote attacker to delete arbitrary user accounts or gain elevated privileges on an affected system.	6.5	More Details
CVE-2020-21048	An issue in the dither.c component of libsixel prior to v1.8.4 allows attackers to cause a denial of service (DOS) via a crafted PNG file.	6.5	More Details
CVE-2021-1878	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina, Security Update 2021-003 Mojave. An attacker in a privileged network position may be able to leak sensitive user information.	6.5	More Details
CVE-2021-40812	The GD Graphics Library (aka LibGD) through 2.3.2 has an out-of-bounds read because of the lack of certain gdGetBuf and gdPutBuf return value checks.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40797	An issue was discovered in the routes middleware in OpenStack Neutron before 16.4.1, 17.x before 17.2.1, and 18.x before 18.1.1. By making API requests involving nonexistent controllers, an authenticated user may cause the API worker to consume increasing amounts of memory, resulting in API performance degradation or denial of service.	6.5	More Details
CVE-2021-30721	A path handling issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. An attacker in a privileged network position may be able to leak sensitive user information.	6.5	More Details
CVE-2021-34785	Multiple vulnerabilities in Cisco BroadWorks CommPilot Application Software could allow an authenticated, remote attacker to delete arbitrary user accounts or gain elevated privileges on an affected system.	6.5	More Details
CVE-2021-3055	An improper restriction of XML external entity (XXE) reference vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator to read any arbitrary file from the file system and send a specifically crafted request to the firewall that causes the service to crash. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.1.10; PAN-OS 10.0 versions earlier than PAN-OS 10.0.6. This issue does not affect Prisma Access.	6.5	More Details
CVE-2020-21081	A cross-site request forgery (CSRF) in Maccms 8.0 causes administrators to add and modify articles without their knowledge via clicking on a crafted URL.	6.5	More Details
CVE-2020-21050	Libsixel prior to v1.8.3 contains a stack buffer overflow in the function gif_process_raster at fromgif.c.	6.5	More Details
CVE-2020-21049	An invalid read in the stb_image.h component of libsixel prior to v1.8.5 allows attackers to cause a denial of service (DOS) via a crafted PSD file.	6.5	More Details
CVE-2021-1860	A memory initialization issue was addressed with improved memory handling. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. A malicious application may be able to disclose kernel memory.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23043	On BIG-IP, on all versions of 16.1.x, 16.0.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x, a directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to access arbitrary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2021-1957	Improper Access Control when ACL link encryption is failed and ACL link is not disconnected during reconnection with paired device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	6.5	More Details
CVE-2021-1960	Improper handling of ASB-C broadcast packets with crafted opcode in LMP can lead to uncontrolled resource consumption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	6.5	More Details
CVE-2021-28567	Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are vulnerable to an Improper Authorization vulnerability in the customers module. Successful exploitation could allow a low-privileged user to modify customer data. Access to the admin console is required for successful exploitation.	6.5	More Details
CVE-2021-1956	Improper handling of ASB-U packet with L2CAP channel ID by slave host can lead to interference with piconet in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	6.5	More Details
CVE-2021-22004	An issue was discovered in SaltStack Salt before 3003.3. The salt minion installer will accept and use a minion config file at C:\salt\conf if that file is in place before the installer is run. This allows for a malicious actor to subvert the proper behaviour of the given minion software.	6.4	More Details
CVE-2021-28499	In Arista's MOS (Metamako Operating System) software which is supported on the 7130 product line, user account passwords set in clear text could leak to users without any password. This issue affects: Arista Metamako Operating System MOS-0.18 and post releases in the MOS-0.1x train All releases in the MOS-0.2x train MOS-0.31.1 and prior releases in the MOS-0.3x train	6.3	More Details
CVE-2021-30714	A race condition was addressed with improved state handling. This issue is fixed in iOS 14.6 and iPadOS 14.6. An application may be able to cause unexpected system termination or write kernel memory.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35526	Backup file without encryption vulnerability is found in Hitachi ABB Power Grids System Data Manager – SDM600 allows attacker to gain access to sensitive information. This issue affects: Hitachi ABB Power Grids System Data Manager – SDM600 1.2 versions prior to FP2 HF6 (Build Nr. 1.2.14002.257).	6.3	More Details
CVE-2021-1929	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	6.2	More Details
CVE-2021-1904	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.2	More Details
CVE-2021-38318	The 3D Cover Carousel WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the id parameter in the ~/cover-carousel.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.	6.1	More Details
CVE-2021-38319	The More From Google WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/morefromgoogle.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.0.2.	6.1	More Details
CVE-2021-38317	The Konnichiwa! Membership WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the plan_id parameter in the ~/views/subscriptions.html.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.8.3.	6.1	More Details
CVE-2021-38339	The Simple Matted Thumbnails WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/simple-matted-thumbnail.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.01.	6.1	More Details
CVE-2021-38336	The Edit Comments XT WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/edit-comments-xt.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38321	The Custom Menu Plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the selected_menu parameter found in the ~/custom-menus.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.3.3.	6.1	More Details
CVE-2021-38340	The Wordpress Simple Shop WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the update_row parameter found in the ~/includes/add_product.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.	6.1	More Details
CVE-2021-38338	The Border Loading Bar WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `f` and `t` parameter found in the ~/titan-framework/iframe-googlefont-preview.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.1.	6.1	More Details
CVE-2021-38316	The WP Academic People List WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the category_name parameter in the ~/admin-panel.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.4.1.	6.1	More Details
CVE-2021-38337	The RSVPMaker Excel WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/phpexcel/PHPExcel/Shared/JAMA/docs/download.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.1.	6.1	More Details
CVE-2021-38320	The simpleSAMLphp Authentication WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/simplesamlphp-authentication.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.7.0.	6.1	More Details
CVE-2020-19855	phpwcms v1.9 contains a cross-site scripting (XSS) vulnerability in /image_zoom.php.	6.1	More Details
CVE-2021-38322	The Twitter Friends Widget WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the pmc_TF_user and pmc_TF_password parameter found in the ~/twitter-friends-widget.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.1.	6.1	More Details
CVE-2021-38323	The RentPress WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the selections parameter found in the ~/src/rentPress/AjaxRequests.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 6.6.4.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35976	The feature to preview a website in Plesk Obsidian 18.0.0 through 18.0.32 on Linux is vulnerable to reflected XSS via the /plesk-site-preview/ PATH, aka PFSI-62467. The attacker could execute JavaScript code in the victim's browser by using the link to preview sites hosted on the server. Authentication is not required to exploit the vulnerability.	6.1	More Details
CVE-2021-38326	The Post Title Counter WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the notice parameter found in the ~/post-title-counter.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.1.	6.1	More Details
CVE-2021-38327	The YouTube Video Inserter WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/adminUI/settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.1.0.	6.1	More Details
CVE-2021-38328	The Notices WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/notices.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 6.1.	6.1	More Details
CVE-2020-19283	A reflected cross-site scripting (XSS) vulnerability in the /newVersion component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML.	6.1	More Details
CVE-2020-19282	A reflected cross-site scripting (XSS) vulnerability in Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the system error message's text field.	6.1	More Details
CVE-2021-38329	The DJ EmailPublish WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/dj-email-publish.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.7.2.	6.1	More Details
CVE-2021-38330	The Yet Another bol.com Plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/yabp.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.4.	6.1	More Details
CVE-2021-38347	The Custom Website Data WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the id parameter found in the ~/views/edit.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.2.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38331	The WP-T-Wap WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the posted parameter found in the ~/wap/writer.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.13.2.	6.1	More Details
CVE-2021-38332	The On Page SEO + Whatsapp Chat Button Plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.1.	6.1	More Details
CVE-2021-38333	The WP Scrippets WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/wp-scrippets.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.5.1.	6.1	More Details
CVE-2021-38334	The WP Design Maps & Places WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the filename parameter found in the ~/wpdmp-admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.	6.1	More Details
CVE-2021-38325	The User Activation Email WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the uae-key parameter found in the ~/user-activation-email.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.3.0.	6.1	More Details
CVE-2021-38335	The Wise Agent Capture Forms WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/WiseAgentCaptureForm.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.	6.1	More Details
CVE-2021-38341	The WooCommerce Payment Gateway Per Category WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/includes/plugin_settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.10.	6.1	More Details
CVE-2018-19957	A vulnerability involving insufficient HTTP security headers has been reported to affect QNAP NAS running QTS, QuTS hero, and QuTScloud. This vulnerability allows remote attackers to launch privacy and security attacks. We have already fixed this vulnerability in the following versions: QTS 4.5.4.1715 build 20210630 and later QuTS hero h4.5.4.1771 build 20210825 and later QuTScloud c4.5.6.1755 build 20210809 and later	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38348	The Advance Search WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the wpas_id parameter found in the ~/inc/admin/views/html-advance-search-admin-options.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.1.2.	6.1	More Details
CVE-2021-33674	Under certain conditions, SAP Contact Center - version 700, does not sufficiently encode user-controlled inputs. This allows an attacker to exploit a Reflected Cross-Site Scripting (XSS) vulnerability when creating a new email and to execute arbitrary code on the victim's browser.	6.1	More Details
CVE-2021-24560	The Software License Manager WordPress plugin before 4.4.8 does not sanitise or escape the edit_record parameter before outputting it back in the page in the admin dashboard, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-30689	A logic issue was addressed with improved state management. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to universal cross site scripting.	6.1	More Details
CVE-2021-1826	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. Processing maliciously crafted web content may lead to universal cross site scripting.	6.1	More Details
CVE-2021-1825	An input validation issue was addressed with improved input validation. This issue is fixed in iTunes 12.11.3 for Windows, iCloud for Windows 12.3, macOS Big Sur 11.3, Safari 14.1, watchOS 7.4, tvOS 14.5, iOS 14.5 and iPadOS 14.5. Processing maliciously crafted web content may lead to a cross site scripting attack.	6.1	More Details
CVE-2021-32202	In CS-Cart version 4.11.1, it is possible to induce copy-paste XSS by manipulating the "post description" filed in the blog post creation page.	6.1	More Details
CVE-2021-33673	Under certain conditions, SAP Contact Center - version 700,does not sufficiently encode user-controlled inputs and persists in them. This allows an attacker to exploit a Stored Cross-Site Scripting (XSS) vulnerability when a user browses through the employee directory and to execute arbitrary code on the victim's browser. Due to the usage of ActiveX in the application, the attacker can further execute operating system level commands.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33675	Under certain conditions, SAP Contact Center - version 700, does not sufficiently encode user-controlled inputs. This allows an attacker to exploit a Reflected Cross-Site Scripting (XSS) vulnerability through phishing and to execute arbitrary code on the victim's browser.	6.1	More Details
CVE-2021-38349	The Integration of Moneybird for WooCommerce WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the error_description parameter found in the ~/templates/wcmb-admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.1.1.	6.1	More Details
CVE-2021-30744	Description: A cross-origin issue with iframe elements was addressed with improved tracking of security origins. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to universal cross site scripting.	6.1	More Details
CVE-2021-23052	On version 14.1.x before 14.1.4.4 and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious user to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.1	More Details
CVE-2021-23041	On BIG-IP version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3, 14.1.x before 14.1.4.2, 13.1.x before 13.1.4.1, and all versions of 12.1.x, a DOM based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the current logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.1	More Details
CVE-2020-21082	A cross-site scripting (XSS) vulnerability in the background administrator article management module of Maccms 8.0 allows attackers to steal administrator and user cookies via crafted payloads in the text fields for Chinese and English names.	6.1	More Details
CVE-2021-39391	Cross Site Scripting (XSS) vulnerability exists in the admin panel in Beego v2.0.1 via the URI path in an HTTP request, which is activated by administrators viewing the "Request Statistics" page.	6.1	More Details
CVE-2021-23027	On version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3.1, and 14.1.x before 14.1.4.3, a DOM based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19515	qdPM V9.1 is vulnerable to Cross Site Scripting (XSS) via qdPM\install\modules\database_config.php.	6.1	More Details
CVE-2021-24510	The MF Gig Calendar WordPress plugin before 1.2 does not sanitise and escape the id GET parameter before outputting back in the admin dashboard when editing an Event, leading to a reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-24508	The Smash Balloon Social Post Feed WordPress plugin before 2.19.2 does not sanitise or escape the feedID POST parameter in its feed_locator AJAX action (available to both authenticated and unauthenticated users) before outputting a truncated version of it in the admin dashboard, leading to an unauthenticated Stored Cross-Site Scripting issue which will be executed in the context of a logged in administrator.	6.1	More Details
CVE-2020-19295	A reflected cross-site scripting (XSS) vulnerability in the /weibo/topic component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML.	6.1	More Details
CVE-2021-38350	The spideranalyse WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the date parameter found in the ~/analyse/index.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.0.1.	6.1	More Details
CVE-2021-38351	The OSD Subscribe WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the osd_subscribe_message parameter found in the ~/options/osd_subscribe_options_subscribers.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.3.	6.1	More Details
CVE-2021-38352	The Feedify – Web Push Notifications WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the feedify_msg parameter found in the ~/includes/base.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.1.8.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38353	The Dropdown and scrollable Text WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the content parameter found in the ~/index.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.	6.1	More Details
CVE-2021-38354	The GNU-Mailman Integration WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the gm_error parameter found in the ~/includes/admin/mailing-lists-page.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.6.	6.1	More Details
CVE-2021-38355	The Bug Library WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the successimportcount parameter found in the ~/bug-library.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.3.	6.1	More Details
CVE-2021-38357	The SMS OVH WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the position parameter found in the ~/sms-ovh-sent.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.1.	6.1	More Details
CVE-2021-38358	The MoolaMojo WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the classes parameter found in the ~/views/button-generator.html.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.7.4.1.	6.1	More Details
CVE-2021-38359	The WordPress InviteBox Plugin for viral Refer-a-Friend Promotions WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the message parameter found in the ~/admin/admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.4.1.	6.1	More Details
CVE-2020-19266	A stored cross-site scripting (XSS) vulnerability in the index.php/Dswjcms/Site/articleList component of Dswjcms 1.6.4 allows attackers to execute arbitrary web scripts or HTML.	6.1	More Details
CVE-2020-19265	A stored cross-site scripting (XSS) vulnerability in the index.php/Dswjcms/Basis/links component of Dswjcms 1.6.4 allows attackers to execute arbitrary web scripts or HTML.	6.1	More Details
CVE-2021-3646	btcpayserver is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34708	Multiple vulnerabilities in image verification checks of Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for Cisco 8000 Series Routers could allow an authenticated, local attacker to execute arbitrary code on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory.	6.0	More Details
CVE-2021-34343	A stack buffer overflow vulnerability has been reported to affect QNAP device running QTS, QuTScloud, QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of QTS, QuTScloud, QuTS hero: QTS 4.5.4.1715 build 20210630 and later QTS 5.0.0.1716 build 20210701 and later QuTScloud c4.5.6.1755 and later QuTS hero h4.5.4.1771 build 20210825 and later	6.0	More Details
CVE-2021-22527	Information leakage vulnerability in NetIQ Access Manager prior to 5.0.1 and 4.5.4	6.0	More Details
CVE-2021-34709	Multiple vulnerabilities in image verification checks of Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for Cisco 8000 Series Routers could allow an authenticated, local attacker to execute arbitrary code on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory.	6.0	More Details
CVE-2021-40824	A logic error in the room key sharing functionality of Element Android before 1.2.2 and matrix-android-sdk2 (aka Matrix SDK for Android) before 1.2.2 allows a malicious Matrix homeserver present in an encrypted room to steal room encryption keys (via crafted Matrix protocol messages) that were originally sent by affected Matrix clients participating in that room. This allows the attacker to decrypt end-to-end encrypted messages sent by affected clients.	5.9	More Details
CVE-2021-30722	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. An attacker in a privileged network position may be able to leak sensitive user information.	5.9	More Details
CVE-2021-30696	An attacker in a privileged network position may be able to misrepresent application state. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A logic issue was addressed with improved state management.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25457	An improper input validation vulnerability in DSP driver prior to SMR Sep-2021 Release 1 allows local attackers to get a limited kernel memory information.	5.9	More Details
CVE-2021-40823	A logic error in the room key sharing functionality of matrix-js-sdk (aka Matrix Javascript SDK) before 12.4.1 allows a malicious Matrix homeserver present in an encrypted room to steal room encryption keys (via crafted Matrix protocol messages) that were originally sent by affected Matrix clients participating in that room. This allows the homeserver to decrypt end-to-end encrypted messages sent by affected clients.	5.9	More Details
CVE-2021-30716	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. An attacker in a privileged network position may be able to perform denial of service.	5.9	More Details
CVE-2021-1884	A race condition was addressed with improved locking. This issue is fixed in Security Update 2021-004 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, Security Update 2021-003 Catalina, tvOS 14.5, macOS Big Sur 11.3. A remote attacker may be able to cause a denial of service.	5.9	More Details
CVE-2020-26300	systeminformation is an npm package that provides system and OS information library for node.js. In systeminformation before version 4.26.2 there is a command injection vulnerability. Problem was fixed in version 4.26.2 with a shell string sanitation fix.	5.9	More Details
CVE-2021-34737	A vulnerability in the DHCP version 4 (DHCPv4) server feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to trigger a crash of the dhcpd process, resulting in a denial of service (DoS) condition. This vulnerability exists because certain DHCPv4 messages are improperly validated when they are processed by an affected device. An attacker could exploit this vulnerability by sending a malformed DHCPv4 message to an affected device. A successful exploit could allow the attacker to cause a NULL pointer dereference, resulting in a crash of the dhcpd process. While the dhcpd process is restarting, which may take up to approximately two minutes, DHCPv4 server services are unavailable on the affected device. This could temporarily prevent network access to clients that join the network during that time period. Note: Only the dhcpd process crashes and eventually restarts automatically. The router does not reload.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28568	Adobe Genuine Services version 7.1 (and earlier) is affected by an Insecure file permission vulnerability during installation process. A local authenticated attacker could leverage this vulnerability to achieve privilege escalation in the context of the current user.	5.8	More Details
CVE-2020-19268	A cross-site request forgery (CSRF) in index.php/Dswjcms/User/tfAdd of Dswjcms 1.6.4 allows authenticated attackers to arbitrarily add administrator users.	5.7	More Details
CVE-2020-29012	An insufficient session expiration vulnerability in FortiSandbox versions 3.2.1 and below may allow an attacker to reuse the unexpired admin user session IDs to gain information about other users configured on the device, should the attacker be able to obtain that session ID (via other, hypothetical attacks)	5.6	More Details
CVE-2021-30791	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 14.7, macOS Big Sur 11.5. Processing a maliciously crafted file may disclose user information.	5.5	More Details
CVE-2021-30695	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted USD file may disclose memory contents.	5.5	More Details
CVE-2021-1739	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in Security Update 2021-002 Catalina, Security Update 2021-003 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. A local user may be able to modify protected parts of the file system.	5.5	More Details
CVE-2021-1740	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in Security Update 2021-002 Catalina, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. A local user may be able to modify protected parts of the file system.	5.5	More Details
CVE-2021-1807	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4. A local user may be able to write arbitrary files.	5.5	More Details
CVE-2021-33365	Memory leak in the gf_isom_get_root_od function in MP4Box in GPAC 1.0.1 allows attackers to read memory via a crafted file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33363	Memory leak in the infe_box_read function in MP4Box in GPAC 1.0.1 allows attackers to read memory via a crafted file.	5.5	More Details
CVE-2021-33361	Memory leak in the afra_box_read function in MP4Box in GPAC 1.0.1 allows attackers to read memory via a crafted file.	5.5	More Details
CVE-2021-32139	The gf_isom_vp_config_get function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-32138	The DumpTrackInfo function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-33366	Memory leak in the gf_isom_oinf_read_entry function in MP4Box in GPAC 1.0.1 allows attackers to read memory via a crafted file.	5.5	More Details
CVE-2021-1846	Processing a maliciously crafted audio file may disclose restricted memory. This issue is fixed in Security Update 2021-002 Catalina, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. An out-of-bounds read was addressed with improved input validation.	5.5	More Details
CVE-2021-33364	Memory leak in the def_parent_box_new function in MP4Box in GPAC 1.0.1 allows attackers to read memory via a crafted file.	5.5	More Details
CVE-2021-1810	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina. A malicious application may bypass Gatekeeper checks.	5.5	More Details
CVE-2021-30782	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.5, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave. A malicious application may be able to access restricted files.	5.5	More Details
CVE-2021-30694	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted USD file may disclose memory contents.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1815	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Big Sur 11.3, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. A local user may be able to modify protected parts of the file system.	5.5	More Details
CVE-2021-30692	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted USD file may disclose memory contents.	5.5	More Details
CVE-2021-1822	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. A local user may be able to modify protected parts of the file system.	5.5	More Details
CVE-2021-30691	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted USD file may disclose memory contents.	5.5	More Details
CVE-2021-1830	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5. A local user may be able to read kernel memory.	5.5	More Details
CVE-2021-1831	The issue was addressed with improved permissions logic. This issue is fixed in iOS 14.5 and iPadOS 14.5. An application may allow shortcuts to access restricted files.	5.5	More Details
CVE-2021-1832	Copied files may not have the expected file permissions. This issue is fixed in Security Update 2021-002 Catalina, iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5, macOS Big Sur 11.3. The issue was addressed with improved permissions logic.	5.5	More Details
CVE-2021-1836	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 14.5 and iPadOS 14.5, tvOS 14.5. A local user may be able to create or modify privileged files.	5.5	More Details
CVE-2021-30697	A logic issue was addressed with improved state management. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. A local user may be able to leak sensitive user information.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30770	A logic issue was addressed with improved validation. This issue is fixed in iOS 14.7, tvOS 14.7, watchOS 7.6. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.	5.5	More Details
CVE-2021-30778	This issue was addressed with improved entitlements. This issue is fixed in macOS Big Sur 11.5. A malicious application may be able to bypass Privacy preferences.	5.5	More Details
CVE-2021-30776	A logic issue was addressed with improved validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-004 Catalina. Playing a malicious audio file may lead to an unexpected application termination.	5.5	More Details
CVE-2021-1930	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	5.5	More Details
CVE-2021-34771	A vulnerability in the Cisco IOS XR Software CLI could allow an authenticated, local attacker to view more information than their privileges allow. This vulnerability is due to insufficient application of restrictions during the execution of a specific command. An attacker could exploit this vulnerability by running a specific command. A successful exploit could allow the attacker to view sensitive configuration information that their privileges might not otherwise allow them to access.	5.5	More Details
CVE-2021-30723	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted USD file may disclose memory contents.	5.5	More Details
CVE-2021-30727	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. A malicious application may be able to modify protected parts of the file system.	5.5	More Details
CVE-2021-30731	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-004 Catalina. An unprivileged application may be able to capture USB devices.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30733	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted font may result in the disclosure of process memory.	5.5	More Details
CVE-2021-30738	A malicious application may be able to overwrite arbitrary files. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-004 Mojave. An issue with path validation logic for hardlinks was addressed with improved path sanitization.	5.5	More Details
CVE-2021-39116	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability in the GIF Image Reader component. The affected versions are before version 8.13.14, and from version 8.14.0 before 8.19.0.	5.5	More Details
CVE-2021-30746	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted USD file may disclose memory contents.	5.5	More Details
CVE-2021-30750	The issue was addressed with improved permissions logic. This issue is fixed in macOS Big Sur 11.3. A malicious application may be able to access the user's recent contacts.	5.5	More Details
CVE-2021-30751	This issue was addressed with improved data protection. This issue is fixed in macOS Big Sur 11.4. A malicious application may be able to bypass certain Privacy preferences.	5.5	More Details
CVE-2021-30709	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted USD file may disclose memory contents.	5.5	More Details
CVE-2021-30753	Processing a maliciously crafted font may result in the disclosure of process memory. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. An out-of-bounds read was addressed with improved input validation.	5.5	More Details
CVE-2021-30706	Processing a maliciously crafted image may lead to disclosure of user information. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. This issue was addressed with improved checks.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30705	This issue was addressed with improved checks. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted ASTC file may disclose memory contents.	5.5	More Details
CVE-2021-36870	Multiple Authenticated Persistent Cross-Site Scripting (XSS) vulnerabilities in WordPress WP Google Maps plugin (versions <= 8.1.12). Vulnerable parameters: &dataset_name, &wpgmza_gdpr_retention_purpose, &wpgmza_gdpr_company_name, &name #2, &name, &polyname #2, &polyname, &address.	5.5	More Details
CVE-2021-36871	Multiple Authenticated Persistent Cross-Site Scripting (XSS) vulnerabilities in WordPress WP Google Maps Pro premium plugin (versions <= 8.1.11). Vulnerable parameters: &wpgmaps_marker_category_name, Value > &attributes[], Name > &attributes[], &icons[], &names[], &description, &link, &title.	5.5	More Details
CVE-2021-30700	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted image may lead to disclosure of user information.	5.5	More Details
CVE-2021-30756	A local attacker may be able to view Now Playing information from the lock screen. This issue is fixed in macOS Big Sur 11.4, iOS 14.6 and iPadOS 14.6. A privacy issue in Now Playing was addressed with improved permissions.	5.5	More Details
CVE-2021-30757	This issue was addressed by enabling hardened runtime. This issue is fixed in iMovie 10.2.4. Entitlements and privacy permissions granted to this app may be used by a malicious app.	5.5	More Details
CVE-2021-30763	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.7, watchOS 7.6. A shortcut may be able to bypass Internet permission requirements.	5.5	More Details
CVE-2021-30768	A logic issue was addressed with improved validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-004 Catalina. A sandboxed process may be able to circumvent sandbox restrictions.	5.5	More Details
CVE-2021-30769	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.7, tvOS 14.7, watchOS 7.6. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30687	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted image may lead to disclosure of user information.	5.5	More Details
CVE-2021-30773	An issue in code signature validation was addressed with improved checks. This issue is fixed in iOS 14.7, tvOS 14.7, watchOS 7.6. A malicious application may be able to bypass code signing checks.	5.5	More Details
CVE-2021-1848	The issue was addressed with improved UI handling. This issue is fixed in iOS 14.5 and iPadOS 14.5. A local user may be able to view sensitive information in the app switcher.	5.5	More Details
CVE-2021-1877	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5. A local user may be able to read kernel memory.	5.5	More Details
CVE-2021-25452	An improper input validation vulnerability in loading graph file in DSP driver prior to SMR Sep-2021 Release 1 allows attackers to perform permanent denial of service on the device.	5.5	More Details
CVE-2021-32135	The trak_box_size function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-25456	OOB read vulnerability in libswmfextractor.so library prior to SMR Sep-2021 Release 1 allows attackers to execute memcpy at arbitrary address via forged wmf file.	5.5	More Details
CVE-2021-30674	This issue was addressed with improved checks. This issue is fixed in iOS 14.6 and iPadOS 14.6. A malicious application may disclose restricted memory.	5.5	More Details
CVE-2021-30658	This issue was addressed with improved handling of file metadata. This issue is fixed in macOS Big Sur 11.3. A malicious application may bypass Gatekeeper checks.	5.5	More Details
CVE-2021-30657	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina. A malicious application may bypass Gatekeeper checks. Apple is aware of a report that this issue may have been actively exploited..	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30682	A logic issue was addressed with improved restrictions. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. A malicious application may be able to leak sensitive user information.	5.5	More Details
CVE-2021-30685	This issue was addressed with improved checks. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Parsing a maliciously crafted audio file may lead to disclosure of user information.	5.5	More Details
CVE-2021-30656	An access issue was addressed with improved memory management. This issue is fixed in iOS 14.5 and iPadOS 14.5. A malicious application may be able to determine kernel memory layout.	5.5	More Details
CVE-2021-30654	This issue was addressed by removing additional entitlements. This issue is fixed in GarageBand 10.4.3. A local attacker may be able to read sensitive information.	5.5	More Details
CVE-2021-32134	The gf_odf_desc_copy function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-32137	Heap buffer overflow in the URL_GetProtocolType function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file.	5.5	More Details
CVE-2021-30673	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina. A malicious application may be able to access a user's call history.	5.5	More Details
CVE-2021-32132	The abst_box_size function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-30669	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A malicious application may bypass Gatekeeper checks.	5.5	More Details
CVE-2021-1883	This issue was addressed with improved checks. This issue is fixed in Security Update 2021-004 Mojave, iOS 14.5 and iPadOS 14.5, watchOS 7.4, Security Update 2021-003 Catalina, tvOS 14.5, macOS Big Sur 11.3. Processing maliciously crafted server messages may lead to heap corruption.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30686	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted audio file may disclose restricted memory.	5.5	More Details
CVE-2021-1852	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5. A local user may be able to read kernel memory.	5.5	More Details
CVE-2021-40223	Rittal CMC PU III Web management (version V3.11.00_2) fails to sanitize user input on several parameters of the configuration (User Configuration dialog, Task Configuration dialog and set logging filter dialog). This allows an attacker to backdoor the device with HTML and browser-interpreted content (such as JavaScript or other client-side scripts). The XSS payload will be triggered when the user accesses some specific sections of the application.	5.4	More Details
CVE-2021-37186	A vulnerability has been identified in LOGO! CMR2020 (All versions < V2.2), LOGO! CMR2040 (All versions < V2.2), SIMATIC RTU3010C (All versions < V4.0.9), SIMATIC RTU3030C (All versions < V4.0.9), SIMATIC RTU3031C (All versions < V4.0.9), SIMATIC RTU3041C (All versions < V4.0.9). The underlying TCP/IP stack does not properly calculate the random numbers used as ISN (Initial Sequence Numbers). An adjacent attacker with network access to the LAN interface could interfere with traffic, spoof the connection and gain access to sensitive information.	5.4	More Details
CVE-2020-19294	A stored cross-site scripting (XSS) vulnerability in the /article/comment component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the article comments section.	5.4	More Details
CVE-2021-33679	The SAP BusinessObjects BI Platform version - 420 allows an attacker, who has basic access to the application, to inject a malicious script while creating a new module document, file, or folder. When another user visits that page, the stored malicious script will execute in their session, hence allowing the attacker to compromise their confidentiality and integrity.	5.4	More Details
CVE-2020-19291	A stored cross-site scripting (XSS) vulnerability in the /weibo/publishdata component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in a posted Weibo.	5.4	More Details
CVE-2021-30667	A logic issue was addressed with improved validation. This issue is fixed in iOS 14.6 and iPadOS 14.6. An attacker in WiFi range may be able to force a client to use a less secure authentication mechanism.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38164	SAP ERP Financial Accounting (RFOPENPOSTING_FR) versions - SAP_APPL - 600, 602, 603, 604, 605, 606, 616, SAP_FIN - 617, 618, 700, 720, 730, SAPSCORE - 125, S4CORE, 100, 101, 102, 103, 104, 105, allows a registered attacker to invoke certain functions that would otherwise be restricted to specific users. These functions are normally exposed over the network and once exploited the attacker may be able to view and modify financial accounting data that only a specific user should have access to.	5.4	More Details
CVE-2021-40377	SmarterTools SmarterMail 16.x before build 7866 has stored XSS. The application fails to sanitize email content, thus allowing one to inject HTML and/or JavaScript into a page that will then be processed and stored by the application.	5.4	More Details
CVE-2021-31274	In LibreNMS < 21.3.0, a stored XSS vulnerability was identified in the API Access page due to insufficient sanitization of the $api->description variable. As a result, arbitrary Javascript code can get executed.	5.4	More Details
CVE-2020-19286	A stored cross-site scripting (XSS) vulnerability in the /question/detail component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the source field of the editor.	5.4	More Details
CVE-2020-19287	A stored cross-site scripting (XSS) vulnerability in the /group/post component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the title.	5.4	More Details
CVE-2021-36695	Deskpro cloud and on-premise Deskpro 2021.1.6 and fixed in Deskpro 2021.1.7 contains a cross-site scripting (XSS) vulnerability in the download file feature on a manager profile due to lack of input validation.	5.4	More Details
CVE-2021-30720	A logic issue was addressed with improved restrictions. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. A malicious website may be able to access restricted ports on arbitrary servers.	5.4	More Details
CVE-2020-19281	A stored cross-site scripting (XSS) vulnerability in the /manage/loginusername component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the username field.	5.4	More Details
CVE-2020-19290	A stored cross-site scripting (XSS) vulnerability in the /weibo/comment component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the Weibo comment section.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19284	A stored cross-site scripting (XSS) vulnerability in the /group/comment component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the group comments text field.	5.4	More Details
CVE-2020-19289	A stored cross-site scripting (XSS) vulnerability in the /member/picture/album component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the new album tab.	5.4	More Details
CVE-2021-29841	IBM Financial Transaction Manager 3.2.4 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: 205045.	5.4	More Details
CVE-2020-19288	A stored cross-site scripting (XSS) vulnerability in the /localhost/u component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in a private message.	5.4	More Details
CVE-2020-19285	A stored cross-site scripting (XSS) vulnerability in the /group/apply component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the Name text field.	5.4	More Details
CVE-2021-24523	The Daily Prayer Time WordPress plugin before 2021.08.10 does not sanitise or escape some of its settings before outputting them in the page, leading to Authenticated Stored Cross-Site Scripting issues.	5.4	More Details
CVE-2020-19292	A stored cross-site scripting (XSS) vulnerability in the /question/ask component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in a posted question.	5.4	More Details
CVE-2021-40347	An issue was discovered in views/list.py in GNU Mailman Postorius before 1.3.5. An attacker (logged into any account) can send a crafted POST request to unsubscribe any user from a mailing list, also revealing whether that address was subscribed in the first place.	5.4	More Details
CVE-2020-19293	A stored cross-site scripting (XSS) vulnerability in the /article/add component of Jeesns 1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in a posted article.	5.4	More Details
CVE-2021-24605	The create_post_page AJAX action of the Custom Post View Generator WordPress plugin through 0.4.6 (available to authenticated user) does not sanitise or escape user input before outputting it back in the response, leading to a Reflected Cross-Site issue	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22524	Injection attack caused the denial of service vulnerability in NetIQ Access Manager prior to 5.0.1 and 4.5.4	5.4	More Details
CVE-2021-24724	The Timetable and Event Schedule by MotoPress WordPress plugin before 2.3.19 does not sanitise some of its parameters, which could allow low privilege users such as author to perform XSS attacks against frontend and backend users when viewing the related event/s	5.4	More Details
CVE-2021-40214	Gibbon v22.0.00 suffers from a stored XSS vulnerability within the wall messages component.	5.4	More Details
CVE-2021-29643	PRTG Network Monitor before 21.3.69.1333 allows stored XSS via an unsanitized string imported from a User Object in a connected Active Directory instance.	5.4	More Details
CVE-2021-38725	Fuel CMS 1.5.0 has a brute force vulnerability in fuel/modules/fuel/controllers/Login.php	5.3	More Details
CVE-2021-23053	On version 15.1.x before 15.1.3, 14.1.x before 14.1.3.1, and 13.1.x before 13.1.3.6, when the brute force protection feature of BIG-IP Advanced WAF or BIG-IP ASM is enabled on a virtual server and the virtual server is under brute force attack, the MySQL database may run out of disk space due to lack of row limit on undisclosed tables in the MYSQL database. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.3	More Details
CVE-2021-20582	IBM Security Secret Server up to 11.0 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 199328.	5.3	More Details
CVE-2021-20569	IBM Security Secret Server up to 11.0 could allow an attacker to enumerate usernames due to improper input validation. IBM X-Force ID: 199243.	5.3	More Details
CVE-2021-33686	Under certain conditions, SAP Business One version - 10.0, allows an unauthorized attacker to get access to some encrypted sensitive information, but does not have control over kind or degree.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23047	On version 16.x before 16.1.0, 15.1.x before 15.1.3.1, 14.1.x before 14.1.4.3, and all versions of 13.1.x, 12.1.x and 11.6.x, when BIG-IP APM performs Online Certificate Status Protocol (OCSP) verification of a certificate that contains Authority Information Access (AIA), undisclosed requests may cause an increase in memory use. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.3	More Details
CVE-2021-1837	A certificate validation issue was addressed. This issue is fixed in iOS 14.5 and iPadOS 14.5. An attacker in a privileged network position may be able to alter network traffic.	5.3	More Details
CVE-2021-36215	LINE client for iOS 10.21.3 and before allows address bar spoofing due to inappropriate address handling.	5.3	More Details
CVE-2021-39122	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view users' emails via an Information Disclosure vulnerability in the /rest/api/2/search endpoint. The affected versions are before version 8.5.13, from version 8.6.0 before 8.13.5, and from version 8.14.0 before 8.15.1.	5.3	More Details
CVE-2021-39200	WordPress is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database. In affected versions output data of the function wp_die() can be leaked under certain conditions, which can include data like nonces. It can then be used to perform actions on your behalf. This has been patched in WordPress 5.8.1, along with any older affected versions via minor releases. It's strongly recommended that you keep auto-updates enabled to receive the fix.	5.3	More Details
CVE-2020-27970	Yandex Browser before 20.10.0 allows remote attackers to spoof the address bar	5.3	More Details
CVE-2019-10941	A vulnerability has been identified in SINEMA Server (All versions < V14 SP3). Missing authentication for functionality that requires administrative user identity could allow an attacker to obtain encoded system configuration backup files. This is only possible through network access to the affected system, and successful exploitation requires no system privileges.	5.3	More Details
CVE-2019-20101	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view whitelist rules via a Broken Access Control vulnerability in the /rest/whitelist/<version>/check endpoint. The affected versions are before version 8.13.3, and from version 8.14.0 before 8.14.1.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37175	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.14.1), RUGGEDCOM ROX RX1400 (All versions < V2.14.1), RUGGEDCOM ROX RX1500 (All versions < V2.14.1), RUGGEDCOM ROX RX1501 (All versions < V2.14.1), RUGGEDCOM ROX RX1510 (All versions < V2.14.1), RUGGEDCOM ROX RX1511 (All versions < V2.14.1), RUGGEDCOM ROX RX1512 (All versions < V2.14.1), RUGGEDCOM ROX RX1524 (All versions < V2.14.1), RUGGEDCOM ROX RX1536 (All versions < V2.14.1), RUGGEDCOM ROX RX5000 (All versions < V2.14.1). The affected devices do not properly handle permissions to traverse the file system. If exploited, an attacker could gain access to an overview of the complete file system on the affected devices.	5.3	More Details
CVE-2021-39118	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to discover the usernames and full names of users via an enumeration vulnerability in the /rest/api/1.0/render endpoint. The affected versions are before version 8.19.0.	5.3	More Details
CVE-2021-39125	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to discover the usernames of users via an enumeration vulnerability in the password reset page. The affected versions are before version 8.5.10, and from version 8.6.0 before 8.13.1.	5.3	More Details
CVE-2021-25453	Some improper access control in Bluetooth APIs prior to SMR Sep-2021 Release 1 allows untrusted application to get Bluetooth information.	5.1	More Details
CVE-2021-1865	An issue obscuring passwords in screenshots was addressed with improved logic. This issue is fixed in iOS 14.5 and iPadOS 14.5. A user's password may be visible on screen.	5.0	More Details
CVE-2021-22239	An unauthorized user was able to insert metadata when creating new issue on GitLab CE/EE 14.0 and later.	5.0	More Details
CVE-2021-23046	On all versions of Guided Configuration before 8.0.0, when a configuration that contains secure properties is created and deployed from Access Guided Configuration (AGC), secure properties are logged in restnoded logs. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40357	A vulnerability has been identified in Teamcenter Active Workspace V4.3 (All versions < V4.3.10), Teamcenter Active Workspace V5.0 (All versions < V5.0.8), Teamcenter Active Workspace V5.1 (All versions < V5.1.5), Teamcenter Active Workspace V5.2 (All versions < V5.2.1). A path traversal vulnerability in the application could allow an attacker to bypass certain restrictions such as direct access to other services within the host.	4.9	More Details
CVE-2021-22526	Open Redirection vulnerability in NetIQ Access Manager prior to 5.0.1 and 4.5.4	4.9	More Details
CVE-2021-21489	SAP NetWeaver Enterprise Portal versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently encode user related data, resulting in Stored Cross-Site Scripting (XSS) vulnerability. This would allow an attacker with administrative privileges to store a malicious script on the portal. The execution of the script content by a victim registered on the portal could compromise the confidentiality and integrity of portal content.	4.8	More Details
CVE-2021-24623	The WordPress Advanced Ticket System, Elite Support Helpdesk WordPress plugin before 1.0.64 does not sanitize or escape form values before saving to the database or when outputting, which allows high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24621	The WP Courses LMS WordPress plugin before 2.0.44 does not sanitise its Video Embed Code, allowing malicious code to be injected in it by high privilege users, even when the unfiltered_html capability is disallowed, which could lead to Stored Cross-Site Scripting issues	4.8	More Details
CVE-2021-24619	The Per page add to head WordPress plugin through 1.4.4 does not properly sanitise one of its setting, allowing malicious HTML to be inserted by high privilege users even when the unfiltered_html capability is disallowed, which could lead to Cross-Site Scripting issues.	4.8	More Details
CVE-2021-24614	The Book appointment online WordPress plugin before 1.39 does not sanitise or escape Service Prices 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-2021-1835	This issue was addressed with improved checks. This issue is fixed in iOS 14.5 and iPadOS 14.5. A person with physical access to an iOS device may be able to access notes from the lock screen.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30702	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A person with physical access to a Mac may be able to bypass Login Window.	4.6	More Details
CVE-2021-30668	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.4. A person with physical access to a Mac may be able to bypass Login Window during a software update.	4.6	More Details
CVE-2021-1928	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	4.6	More Details
CVE-2021-30699	A window management issue was addressed with improved state management. This issue is fixed in iOS 14.6 and iPadOS 14.6. A user may be able to view restricted content from the lockscreen.	4.6	More Details
CVE-2021-25450	Path traversal vulnerability in FactoryAirCommnadManger prior to SMR Sep-2021 Release 1 allows attackers to write file as system uid via remote socket.	4.5	More Details
CVE-2021-39212	ImageMagick is free software delivered as a ready-to-run binary distribution or as source code that you may use, copy, modify, and distribute in both open and proprietary applications. In affected versions and in certain cases, Postscript files could be read and written when specifically excluded by a `module` policy in `policy.xml`. ex. <policy domain="module" rights="none" pattern="PS" />. The issue has been resolved in ImageMagick 7.1.0-7 and in 6.9.12-22. Fortunately, in the wild, few users utilize the `module` policy and instead use the `coder` policy that is also our workaround recommendation: <policy domain="coder" rights="none" pattern="{PS,EPI,EPS,EPSF,EPSI}" />.	4.4	More Details
CVE-2021-1824	This issue was addressed with improved entitlements. This issue is fixed in macOS Big Sur 11.3, Security Update 2021-002 Catalina. A malicious application with root privileges may be able to access private information.	4.4	More Details
CVE-2021-28497	In Arista's MOS (Metamako Operating System) software which is supported on the 7130 product line, under certain conditions, the bash shell might be accessible to unprivileged users in situations where they should not have access. This issue affects: Arista Metamako Operating System All releases in the MOS-0.1x train MOS-0.26.6 and below releases in the MOS-0.2x train MOS-0.31.1 and below releases in the MOS-0.3x train	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33011	All versions of the afffected TOYOPUC-PC10 Series,TOYOPUC-Plus Series,TOYOPUC-PC3J/PC2J Series, TOYOPUC-Nano Series products may not be able to properly process an ICMP flood, which may allow an attacker to deny Ethernet communications between affected devices.	4.3	More Details
CVE-2021-28569	Adobe Media Encoder version 15.1 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4.3	More Details
CVE-2021-24431	The Language Bar Flags WordPress plugin through 1.0.8 does not have any CSRF in place when saving its settings and did not sanitise or escape them when generating the flag bar in the frontend. This could allow attackers to make a logged in admin change the settings, and set Cross-Site Scripting payload in them, which will be executed in the frontend for all users	4.3	More Details
CVE-2021-33981	An insecure, direct object vulnerability in hunting/fishing license retrieval function of the "Fish | Hunt FL" iOS app versions 3.8.0 and earlier allows a remote authenticated attacker to retrieve other people's personal information and images of their hunting/fishing licenses.	4.3	More Details
CVE-2021-1854	A call termination issue with was addressed with improved logic. This issue is fixed in iOS 14.5 and iPadOS 14.5. A legacy cellular network can automatically answer an incoming call when an ongoing call ends or drops. .	4.3	More Details
CVE-2021-24725	The Comment Link Remove and Other Comment Tools WordPress plugin before 2.1.6 does not have CSRF check in its 'Delete comments easily', which could allow attackers to make logged in admin delete arbitrary comments	4.3	More Details
CVE-2021-1872	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, macOS Big Sur 11.3. Muting a CallKit call while ringing may not result in mute being enabled.	4.3	More Details
CVE-2021-39121	Affected versions of Atlassian Jira Server and Data Center allow authenticated remote attackers to enumerate the keys of private Jira projects via an Information Disclosure vulnerability in the /rest/api/latest/projectvalidate/key endpoint. The affected versions are before version 8.5.18, from version 8.6.0 before 8.13.10, and from version 8.14.0 before 8.18.2.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24586	The Per page add to head WordPress plugin before 1.4.4 is lacking any CSRF check when saving its settings, which could allow attackers to make a logged in admin change them. Furthermore, as the plugin allows arbitrary HTML to be inserted in one of the setting (feature mentioned by the plugin), this could lead to Stored XSS issue which will be triggered either in the backend, frontend or both depending on the payload used.	4.3	More Details
CVE-2021-20508	IBM Security Secret Server up to 11.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 199322.	4.3	More Details
CVE-2021-39124	The Cross-Site Request Forgery (CSRF) failure retry feature of Atlassian Jira Server and Data Center before version 8.16.0 allows remote attackers who are able to trick a user into retrying a request to bypass CSRF protection and replay a crafted request.	4.3	More Details
CVE-2020-27940	This issue was addressed with improved file handling. This issue is fixed in Apple TV app for Fire OS 6.1.0.6A142:7.1.0. An attacker with file system access may modify scripts used by the app.	4.3	More Details
CVE-2021-21103	Adobe Illustrator version 25.2 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4.3	More Details
CVE-2021-1861	An issue existed in determining cache occupancy. The issue was addressed through improved logic. This issue is fixed in macOS Big Sur 11.3. A malicious website may be able to track users by setting state in a cache.	4.3	More Details
CVE-2021-37191	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0 SP2). An unauthenticated attacker in the same network of the affected system could brute force the usernames from the affected software.	4.3	More Details
CVE-2021-37192	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0 SP2). The affected software has an information disclosure vulnerability that could allow an attacker to retrieve a list of network devices a known user can manage.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37193	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0 SP2). An unauthenticated attacker in the same network of the affected system could manipulate certain parameters and set a valid user of the affected software as invalid (or vice-versa).	4.3	More Details
CVE-2021-30718	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.4. A non-privileged user may be able to modify restricted settings.	4.3	More Details
CVE-2021-37532	SAP Business One version - 10, due to improper input validation, allows an authenticated User to gain access to directory and view the contents of index in the directory, which would otherwise be restricted to high privileged User.	4.3	More Details
CVE-2021-37190	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0 SP2). The affected software has an information disclosure vulnerability that could allow an attacker to retrieve VPN connection for a known user.	4.3	More Details
CVE-2021-33688	SAP Business One allows an attacker with business privileges to execute crafted database queries, exposing the back-end database. Due to framework restrictions, only some information can be obtained.	4.3	More Details
CVE-2021-25459	An improper access control vulnerability in sspInit() in BlockchainTZService prior to SMR Sep-2021 Release 1 allows attackers to start BlockchainTZService.	4.0	More Details
CVE-2021-25460	An improper access control vulnerability in sspExit() in BlockchainTZService prior to SMR Sep-2021 Release 1 allows attackers to terminate BlockchainTZService.	4.0	More Details
CVE-2021-25461	An improper length check in APAService prior to SMR Sep-2021 Release 1 results in stack based Buffer Overflow.	4.0	More Details
CVE-2021-25463	Improper access control vulnerability in PENUP prior to version 3.8.00.18 allows arbitrary webpage loading in webview.	4.0	More Details
CVE-2021-28566	Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are vulnerable to an Information Disclosure vulnerability when uploading a modified png file to a product image. Successful exploitation could lead to the disclosure of document root path by an unauthenticated attacker. Access to the admin console is required for successful exploitation.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25464	An improper file management vulnerability in SamsungCapture prior to version 4.8.02 allows sensitive information leak.	3.3	More Details
CVE-2021-37176	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). The femap.exe application lacks proper validation of user-supplied data when parsing modfem files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14260)	3.3	More Details
CVE-2021-30671	A validation issue was addressed with improved logic. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina. A malicious application may be able to send unauthorized Apple events to Finder.	3.3	More Details
CVE-2021-30803	A permissions issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.5. A malicious application may be able to access a user's recent Contacts.	3.3	More Details
CVE-2021-25455	OOB read vulnerability in libsaviextractor.so library prior to SMR Sep-2021 Release 1 allows attackers to access arbitrary address through pointer via forged avi file.	3.3	More Details
CVE-2021-25451	A PendingIntent hijacking in NetworkPolicyManagerService prior to SMR Sep-2021 Release 1 allows attackers to get IMSI data.	3.3	More Details
CVE-2021-25458	NULL pointer dereference vulnerability in ION driver prior to SMR Sep-2021 Release 1 allows attackers to cause memory corruption.	3.3	More Details
CVE-2021-30804	A permissions issue was addressed with improved validation. This issue is fixed in iOS 14.7. A malicious application may be able to access Find My data.	3.3	More Details
CVE-2021-25462	NULL pointer dereference vulnerability in NPU driver prior to SMR Sep-2021 Release 1 allows attackers to cause memory corruption.	3.3	More Details
CVE-2021-25465	An improper scheme check vulnerability in Samsung Themes prior to version 5.2.01 allows attackers to perform Man-in-the-middle attack.	3.3	More Details
CVE-2021-25454	OOB read vulnerability in libsaacextractor.so library prior to SMR Sep-2021 Release 1 allows attackers to execute remote DoS via forged aac file.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40537	Server Side Request Forgery (SSRF) vulnerability exists in owncloud/user_ldap < 0.15.4 in the settings of the user_ldap app. Administration role is necessary for exploitation.	2.7	More Details
CVE-2021-3049	An improper authorization vulnerability in the Palo Alto Networks Cortex XSOAR server enables an authenticated network-based attacker with investigation read permissions to download files from incident investigations of which they are aware but are not a part of. This issue impacts: All Cortex XSOAR 5.5.0 builds; Cortex XSOAR 6.1.0 builds earlier than 12099345. This issue does not impact Cortex XSOAR 6.2.0 versions.	2.6	More Details
CVE-2021-1862	Description: A person with physical access may be able to access contacts. This issue is fixed in iOS 14.5 and iPadOS 14.5. Impact: An issue with Siri search access to information was addressed with improved logic.	2.4	More Details
CVE-2021-1863	An issue existed with authenticating the action triggered by an NFC tag. The issue was addressed with improved action authentication. This issue is fixed in iOS 14.5 and iPadOS 14.5. A person with physical access to an iOS device may be able to place phone calls to any phone number.	2.4	More Details
CVE-2021-28581	Adobe Creative Cloud Desktop 3.5 (and earlier) is affected by an uncontrolled search path vulnerability that could result in elevation of privileges. Exploitation of this issue requires user interaction in that a victim must log on to the attacker's local machine.	N/A	More Details
CVE-2021-37418	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-31874. Reason: This candidate is a reservation duplicate of CVE-2021-31874. Notes: All CVE users should reference CVE-2021-31874 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-28732	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-28372. Reason: This candidate is a duplicate of CVE-2021-28372. A typo caused the wrong ID to be used. Notes: All CVE users should reference CVE-2021-28372 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details