SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 15 April 2020

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-2020-1614	A Use of Hard-coded Credentials vulnerability exists in the NFX250 Series for the vSRX Virtual Network Function (VNF) instance, which allows an attacker to take control of the vSRX VNF instance if they have the ability to access an administrative service (e.g. SSH) on the VNF, either locally, or through the network. This issue only affects the NFX250 Series vSRX VNF. No other products or platforms are affected. This issue is only applicable to environments where the vSRX VNF root password has not been configured. This issue affects the Juniper Networks NFX250 Network Services Platform vSRX VNF instance on versions prior to 19.2R1.	10.0	More Details
CVE-2020-11543	OpsRamp Gateway before 7.0.0 has a backdoor account vadmin with the password 9vt@f3Vt that allows root SSH access to the server. This issue has been resolved in OpsRamp Gateway firmware version 7.0.0 where an administrator and a system user accounts are the only available user accounts for the gateway appliance.	9.8	More Details
CVE-2020-11630	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. In several sections of code, the verification of serialized objects sent between nodes (connected via the Peers protocol) allows insecure objects to be deserialized.	9.8	More Details
CVE-2018-21075	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. The Call+ application can load classes from an unintended path, leading to Code Execution. The Samsung ID is SVE-2017-10886 (April 2018).	9.8	More Details
CVE-2020-10980	GitLab EE/CE 8.0.rc1 to 12.9 is vulnerable to a blind SSRF in the FogBugz integration.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1615	The factory configuration for vMX installations, as shipped, includes default credentials for the root account. Without proper modification of these default credentials by the administrator, an attacker could exploit these credentials and access the vMX instance without authorization. This issue affects Juniper Networks Junos OS: 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on vMX; 17.2 versions prior to 17.2R3-S3 on vMX; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on vMX; 17.4 versions prior to 17.4R2-S9, 17.4R3 on vMX; 18.1 versions prior to 18.1R3-S9 on vMX; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on vMX; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D60 on vMX; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on vMX; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on vMX; 19.1 versions prior to 19.1R1-S4, 19.1R2, 19.1R3 on vMX; 19.2 versions prior to 19.2R1-S3, 19.2R2 on vMX; 19.3 versions prior to 19.3R1-S1, 19.3R2 on vMX.	9.8	More Details
CVE-2020-11656	In SQLite through 3.31.1, the ALTER TABLE implementation has a use-after-free, as demonstrated by an ORDER BY clause that belongs to a compound SELECT statement.	9.8	More Details
CVE-2020-10621	Multiple issues exist that allow files to be uploaded and executed on the WebAccess/NMS (versions prior to 3.0.2).	9.8	More Details
CVE-2020-10625	WebAccess/NMS (versions prior to 3.0.2) allows an unauthenticated remote user to create a new admin account.	9.8	More Details
CVE-2020-10631	An attacker could use a specially crafted URL to delete or read files outside the WebAccess/NMS's (versions prior to 3.0.2) control.	9.8	More Details
CVE-2020-8961	An issue was discovered in Avira Free-Antivirus before 15.0.2004.1825. The Self-Protection feature does not prohibit a write operation from an external process. Thus, code injection can be used to turn off this feature. After that, one can construct an event that will modify a file at a specific location, and pass this event to the driver, thereby defeating the anti-virus functionality.	9.8	More Details
CVE-2020-3952	Under certain conditions, vmdir that ships with VMware vCenter Server, as part of an embedded or external Platform Services Controller (PSC), does not correctly implement access controls.	9.8	More Details
CVE-2015-5524	An issue was discovered on Samsung mobile devices with KK(4.4) and later software through 2015-05-13. There is a buffer overflow in datablock_write because the amount of received data is not validated. The Samsung ID is SVE-2015-4018 (December 2015).	9.8	More Details
CVE-2015-8546	An issue was discovered on Samsung mobile devices with software through 2015-11-12, affecting the Galaxy S6/S6 Edge, Galaxy S6 Edge+, and Galaxy Note5 with the Shannon333 chipset. There is a stack-based buffer overflow in the baseband process that is exploitable for remote code execution via a fake base station. The Samsung ID is SVE-2015-5123 (December 2015).	9.8	More Details
CVE-2020-11705	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. /ajax/ImportCertificate allows an attacker to load an arbitrary certificate in .pfx format or overwrite arbitrary files via the fileName parameter.	9.8	More Details
CVE-2020-11708	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. Privilege escalation can occur via the /ajax/SetUserInfo messages parameter because of the EXECUTE() feature, which is for executing programs when certain events are triggered.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11710	An issue was discovered in docker-kong (for Kong) through 2.0.3. The admin API port may be accessible on interfaces other than 127.0.0.1. NOTE: The vendor argue that this CVE is not a vulnerability because it has an inaccurate bug scope and patch links. “1) Inaccurate Bug Scope - The issue scope was on Kong's docker-compose template, and not Kong's docker image itself. In reality, this issue is not associated with any version of the Kong gateway. As such, the description stating ‘An issue was discovered in docker-kong (for Kong) through 2.0.3.’ is incorrect. This issue only occurs if a user decided to spin up Kong via docker-compose without following the security documentation. The docker-compose template is meant for users to quickly get started with Kong, and is meant for development purposes only. 2) Incorrect Patch Links - The CVE currently points to a documentation improvement as a “Patch” link: https://github.com/Kong/docs.konghq.com/commit/d693827c32144943a2f45abc017c1321b33ff611.This link actually points to an improvement Kong Inc made for fool-proofing. However, instructions for how to protect the admin API were already well-documented here: https://docs.konghq.com/2.0.x/secure-admin-api/#network-layer-access-restrictions , which was first published back in 2017 (as shown in this commit: https://github.com/Kong/docs.konghq.com/commit/e99cf875d875dd84fdb751079ac37882c9972949) Lastly, the hyperlink to https://github.com/Kong/kong (an unrelated Github Repo to this issue) on the Hyperlink list does not include any meaningful information on this topic.	9.8	More Details
CVE-2020-11722	Dungeon Crawl Stone Soup (aka DCSS or crawl) before 0.25 allows remote attackers to execute arbitrary code via Lua bytecode embedded in an uploaded .crawlrc file.	9.8	More Details
CVE-2020-11673	An issue was discovered in the Responsive Poll through 1.3.4 for Wordpress. It allows an unauthenticated user to manipulate polls, e.g., delete, clone, or view a hidden poll. This is due to the usage of the callback wp_ajax_nopriv function in Includes/Total-Soft-Poll-Ajax.php for sensitive operations.	9.8	More Details
CVE-2019-16879	The Synergy Systems & Solutions (SSS) HUSKY RTU 6049-E70, with firmware Versions 5.0 and prior, has a Missing Authentication for Critical Function (CWE-306) vulnerability. The affected product does not require authentication for TELNET access, which may allow an attacker to change configuration or perform other malicious activities.	9.8	More Details
CVE-2020-10383	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is an unauthenticated remote code execution in the com_mb24sysapi module.	9.8	More Details
CVE-2019-10939	A vulnerability has been identified in TIM 3V-IE (incl. SIPLUS NET variants) (All versions < V2.8), TIM 3V-IE Advanced (incl. SIPLUS NET variants) (All versions < V2.8), TIM 3V-IE DNP3 (incl. SIPLUS NET variants) (All versions < V3.3), TIM 4R-IE (incl. SIPLUS NET variants) (All versions < V2.8), TIM 4R-IE DNP3 (incl. SIPLUS NET variants) (All versions < V3.3). The affected versions contain an open debug port that is available under certain specific conditions. The vulnerability is only available if the IP address is configured to 192.168.1.2. If available, the debug port could be exploited by an attacker with network access to the device. No user interaction is required to exploit this vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the affected device. At the stage of publishing this security advisory no public exploitation is known.	9.8	More Details
CVE-2020-6195	SAP Business Objects Business Intelligence Platform (CMC), version 4.1, 4.2, shows cleartext password in the response, leading to Information Disclosure. It involves social engineering in order to gain access to system and If password is known, it would give administrative rights to the attacker to read/modify delete the data and rights within the system.	9.8	More Details
CVE-2018-21072	An issue was discovered on Samsung mobile devices with M(6.0), N(7.x), and O(8.0) (Exynos chipsets) software. A kernel driver allows out-of-bounds Read/Write operations and possibly arbitrary code execution. The Samsung ID is SVE-2018-11358 (May 2018).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21066	An issue was discovered on Samsung mobile devices with M(6.0) (Exynos or MediaTek chipsets) software. There is a buffer overflow in a Trustlet that can cause memory corruption. The Samsung ID is SVE-2018-11599 (July 2018).	9.8	More Details
CVE-2018-21065	An issue was discovered on Samsung mobile devices with M(6.0), N(7.x), and O(8.x) software. There is an integer underflow in eCryptFS because of a missing size check. The Samsung ID is SVE-2017-11855 (August 2018).	9.8	More Details
CVE-2018-21044	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.0) software. The sem Trustlet has a buffer overflow that leads to arbitrary TEE code execution. The Samsung IDs are SVE-2018-13230, SVE-2018-13231, SVE-2018-13232, SVE-2018-13233 (December 2018).	9.8	More Details
CVE-2017-18644	An issue was discovered on Samsung mobile devices with L(5.1), M(6.x), and N(7.x) software. There is a muic_set_reg_sel heap-based buffer overflow during the reading of MUIC register values. The Samsung ID is SVE-2017-10011 (December 2017).	9.8	More Details
CVE-2017-18645	An issue was discovered on Samsung mobile devices with M(6.x) and N(7.x) (Qualcomm chipsets) software. There is a panel_lpm sysfs stack-based buffer overflow. The Samsung ID is SVE-2017-9414 (December 2017).	9.8	More Details
CVE-2018-21089	An issue was discovered on Samsung mobile devices with N(7.x) (MT6755/MT6757 Mediatek models) software. Bootloader has an integer overflow that leads to arbitrary code execution via the download offset control. The Samsung ID is SVE-2017-10732 (January 2018).	9.8	More Details
CVE-2018-21090	An issue was discovered on Samsung mobile devices with software through 2017-11-03 (S.LSI modem chipsets). The Exynos modem chipset has a baseband buffer overflow. The Samsung ID is SVE-2017-10745 (January 2018).	9.8	More Details
CVE-2018-21087	An issue was discovered on Samsung mobile devices with L(5.x), M(6.x), and N(7.x) software. There is a vnswap heap-based buffer overflow via the store function, with resultant privilege escalation. The Samsung ID is SVE-2017-10599 (January 2018).	9.8	More Details
CVE-2020-11600	An issue was discovered on Samsung mobile devices with Q(10.0) software. There is arbitrary code execution in the Fingerprint Trustlet via a memory overwrite. The Samsung IDs are SVE-2019-16587, SVE-2019-16588, SVE-2019-16589 (April 2020).	9.8	More Details
CVE-2020-11603	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (incorporating TEEGRIS) software. Type confusion in the MLDAP Trustlet allows arbitrary code execution. The Samsung ID is SVE-2020-16599 (April 2020).	9.8	More Details
CVE-2018-21038	An issue was discovered on Samsung mobile devices with N(7.x) software. The Secure Folder app's startup logic allows authentication bypass. The Samsung ID is SVE-2018-11628 (December 2018).	9.8	More Details
CVE-2018-21064	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. There is an array overflow in a driver's input booster. The Samsung ID is SVE-2017-11816 (August 2018).	9.8	More Details
CVE-2018-21042	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. Dual Messenger allows installation of an arbitrary APK with resultant privileged code execution. The Samsung ID is SVE-2018-13299 (December 2018).	9.8	More Details
CVE-2018-21049	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.X) (Exynos chipsets) software. There is an arbitrary memory write in a Trustlet because a secure driver allows access to sensitive APIs. The Samsung ID is SVE-2018-12881 (November 2018).	9.8	More Details
CVE-2018-21050	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.X) (Exynos chipsets) software. There is a Buffer overflow in the esecomm Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2018-12852 (October 2018).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21051	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) (Exynos chipsets) software. There is an invalid free in the fingerprint Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2018-12853 (October 2018).	9.8	More Details
CVE-2018-21052	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.X) (Exynos chipsets) software. There is incorrect usage of shared memory in the vaultkeeper Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2018-12855 (October 2018).	9.8	More Details
CVE-2018-21054	An issue was discovered on Samsung mobile devices with M(6.0), N(7.x) and O(8.x) except exynos9610/9820 in all Platforms, M(6.0) except MSM8909 SC77xx/9830 exynos3470/5420, N(7.0) except MSM8939, N(7.1) except MSM8996 SDM6xx/M6737T software. There is an integer underflow with a resultant buffer overflow in eCryptFS. The Samsung ID is SVE-2017-11857 (September 2018).	9.8	More Details
CVE-2018-21055	An issue was discovered on Samsung mobile devices with N(7.0) (Qualcomm models using MSM8996 chipsets) software. A device can be rooted with a custom image to execute arbitrary scripts in the INIT context. The Samsung ID is SVE-2018-11940 (September 2018).	9.8	More Details
CVE-2018-21057	An issue was discovered on Samsung mobile devices with N(7.x) O(8.x, and P(9.0) (Exynos chipsets) software. There is a stack-based buffer overflow in the Shannon Baseband. The Samsung ID is SVE-2018-12757 (September 2018).	9.8	More Details
CVE-2018-21058	An issue was discovered on Samsung mobile devices with N(7.0), O(8.0) (exynos7420 or Exynos 8890/8996 chipsets) software. Cache attacks can occur against the Keymaster AES-GCM implementation because T-Tables are used; the Cryptography Extension (CE) is not used. The Samsung ID is SVE-2018-12761 (September 2018).	9.8	More Details
CVE-2018-21063	An issue was discovered on Samsung mobile devices with M(6.0), N(7.x), and O(8.x) (Exynos chipsets) software. Keymaster has an architectural problem because tlApi in TEE is not properly protected. The Samsung ID is SVE-2018-11792 (August 2018).	9.8	More Details
CVE-2020-6238	SAP Commerce, versions - 6.6, 6.7, 1808, 1811, 1905, does not process XML input securely in the Rest API from Servlet xyformsweb, leading to Missing XML Validation. This affects confidentiality and availability (partially) of SAP Commerce.	9.3	More Details
CVE-2020-5260	Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. Git uses external "credential helper" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that contain an encoded newline can inject unintended values into the credential helper protocol stream, causing the credential helper to retrieve the password for one server (e.g., good.example.com) for an HTTP request being made to another server (e.g., evil.example.com), resulting in credentials for the former being sent to the latter. There are no restrictions on the relationship between the two, meaning that an attacker can craft a URL that will present stored credentials for any host to a host of their choosing. The vulnerability can be triggered by feeding a malicious URL to git clone. However, the affected URLs look rather suspicious; the likely vector would be through systems which automatically clone URLs not visible to the user, such as Git submodules, or package systems built around Git. The problem has been patched in the versions published on April 14th, 2020, going back to v2.17.x. Anyone wishing to backport the change further can do so by applying commit 9a6bbee (the full release includes extra checks for git fsck, but that commit is sufficient to protect clients against the vulnerability). The patched versions are: 2.17.4, 2.18.3, 2.19.4, 2.20.3, 2.21.2, 2.22.3, 2.23.2, 2.24.2, 2.25.3, 2.26.1.	9.3	More Details
CVE-2020-11604	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (incorporating TEEGRIS) software. There is an Out-of-bounds read in the MLDAP Trustlet. The Samsung ID is SVE-2019-16565 (April 2020).	9.1	More Details
CVE-2020-10619	An attacker could use a specially crafted URL to delete files outside the WebAccess/NMS's (versions prior to 3.0.2) control.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21081	An issue was discovered on Samsung mobile devices with N(7.x) software. In Dual Messenger, the second app can use the runtime permissions of the first app without a user's consent. The Samsung ID is SVE-2017-11018 (March 2018).	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-6452	Heap buffer overflow in media in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-4362	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional is vulnerable to a privilege escalation vulnerability when using token-based authentication in an admin request over the SOAP connector. IBM X-Force ID: 178929.	8.8	More Details
CVE-2020-6448	Use after free in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6450	Use after free in WebAudio in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6451	Use after free in WebAudio in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6454	Use after free in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.	8.8	More Details
CVE-2020-6455	Out of bounds read in WebSQL in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6423	Use after free in audio in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6430	Type Confusion in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-10603	WebAccess/NMS (versions prior to 3.0.2) does not properly sanitize user input and may allow an attacker to inject system commands remotely.	8.8	More Details
CVE-2020-6434	Use after free in devtools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6219	SAP Business Objects Business Intelligence Platform (CrystalReports WebForm Viewer), versions 4.1, 4.2, and Crystal Reports for VS version 2010, allows an attacker with basic authorization to perform deserialization attack in the application, leading to service interruptions and denial of service and unauthorized execution of arbitrary commands, leading to Deserialization of Untrusted Data.	8.8	More Details
CVE-2020-11553	An issue was discovered in Castle Rock SNMPc Online 12.10.10 before 2020-01-28. There is pervasive CSRF.	8.8	More Details
CVE-2020-6436	Use after free in window management in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6439	Insufficient policy enforcement in navigations in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass security UI via a crafted HTML page.	8.8	More Details
CVE-2020-9478	An issue was discovered in Rubrik 5.0.3-2296. An OS command injection vulnerability allows an authenticated attacker to remotely execute arbitrary code on Rubrik-managed systems.	8.8	More Details
CVE-2019-18822	A privilege escalation vulnerability in ZOOM Call Recording 6.3.1 allows its user account (i.e., the account under which the program runs - by default, the callrec account) to elevate privileges to root by abusing the callrec-rs@.service. The callrec-rs@.service starts the /opt/callrec/bin/rs binary with root privileges, and this binary is owned by callrec. It can be replaced by a Trojan horse.	8.8	More Details
CVE-2020-10382	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is an authenticated remote code execution in the backup-scheduler.	8.8	More Details
CVE-2020-6443	Insufficient data validation in developer tools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had convinced the user to use devtools to execute arbitrary code via a crafted HTML page.	8.8	More Details
CVE-2020-9004	A remote authenticated authorization-bypass vulnerability in Wowza Streaming Engine 4.8.0 and earlier allows any read-only user to issue requests to the administration panel in order to change functionality. For example, a read-only user may activate the Java JMX port in unauthenticated mode and execute OS commands under root privileges. This issue was resolved in Wowza Streaming Engine 4.8.5.	8.8	More Details
CVE-2020-5739	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges.	8.8	More Details
CVE-2020-5738	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface.	8.8	More Details
CVE-2019-13916	An issue was discovered in Cypress (formerly Broadcom) WICED Studio 6.2 CYW20735B1 and CYW20819A1. As a Bluetooth Low Energy (BLE) packet is received, it is copied into a Heap (ThreadX Block) buffer. The buffer allocated in dhmulp_getRxBuffer is four bytes too small to hold the maximum of 255 bytes plus headers. It is possible to corrupt a pointer in the linked list holding the free buffers of the g_mm_BLEDeviceToHostPool Block pool. This pointer can be fully controlled by overflowing with 3 bytes of packet data and the first byte of the packet CRC checksum. The checksum can be freely chosen by adapting the packet data accordingly. An attacker might be able to allocate the overwritten address as a receive buffer resulting in a write-what-where condition. This is fixed in BT SDK2.4 and BT SDK2.45.	8.8	More Details
CVE-2020-11741	An issue was discovered in xenoprof in Xen through 4.13.x, allowing guest OS users (with active profiling) to obtain sensitive information about other guests, cause a denial of service, or possibly gain privileges. For guests for which "active" profiling was enabled by the administrator, the xenoprof code uses the standard Xen shared ring structure. Unfortunately, this code did not treat the guest as a potential adversary: it trusts the guest not to modify buffer size information or modify head / tail pointers in unexpected ways. This can crash the host (DoS). Privilege escalation cannot be ruled out.	8.8	More Details
CVE-2020-6447	Inappropriate implementation in developer tools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had convinced the user to use devtools to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9384	An Insecure Direct Object Reference (IDOR) vulnerability in the Change Password feature of Subex ROC Partner Settlement 10.5 allows remote authenticated users to achieve account takeover via manipulation of POST parameters. NOTE: This vulnerability may only affect a testing version of the application	8.8	More Details
CVE-2020-5549	Cross-site request forgery (CSRF) vulnerability in EasyBlocks IPv6 Ver. 2.0.1 and earlier and Enterprise Ver. 2.0.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	8.8	More Details
CVE-2020-5735	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code.	8.8	More Details
CVE-2020-6225	SAP NetWeaver (Knowledge Management), versions (KMC-CM - 7.00, 7.01, 7.02, 7.30, 7.31, 7.40, 7.50 and KMC-WPC 7.30, 7.31, 7.40, 7.50), does not sufficiently validate path information provided by users, thus characters representing traverse to parent directory are passed through to the file APIs, allowing the attacker to overwrite, delete, or corrupt arbitrary files on the remote server, leading to Path Traversal.	8.8	More Details
CVE-2019-15789	Privilege escalation vulnerability in MicroK8s allows a low privilege user with local access to obtain root access to the host by provisioning a privileged container. Fixed in MicroK8s 1.15.3.	8.8	More Details
CVE-2020-11707	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. It doesn't enforce permission over Windows Symlinks or Junctions. As a result, a low-privileged user (non-admin) can craft a Junction Link in a directory he has full control of, breaking out of the sandbox.	8.8	More Details
CVE-2020-11706	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. The Admin Interface allows CSRF for actions such as: Change any username and password, admin ones included; Create/Delete users; Enable/Disable Services; Set a rogue update proxy; and Shutdown the server.	8.8	More Details
CVE-2020-8828	As of v1.5.0, the default admin password is set to the argocd-server pod name. For insiders with access to the cluster or logs, this issue could be abused for privilege escalation, as Argo has privileged roles. A malicious insider is the most realistic threat, but pod names are not meant to be kept secret and could wind up just about anywhere.	8.8	More Details
CVE-2020-11701	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. CSRF exists in the User Web Interface, as demonstrated by granting filesystem access to the public for uploading and deleting files and directories.	8.8	More Details
CVE-2020-11627	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. A Cross Site Request Forgery (CSRF) issue has been found in the CA UI.	8.8	More Details
CVE-2020-6235	SAP Solution Manager (Diagnostics Agent), version 7.2, does not perform the authentication check for the functionalities of the Collector Simulator, leading to Missing Authentication.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1613	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20.	8.6	More Details
CVE-2019-11480	The pc-kernel snap build process hardcoded the --allow-insecure-repositories and --allow-unauthenticated apt options when creating the build chroot environment. This could allow an attacker who is able to perform a MITM attack between the build environment and the Ubuntu archive to install a malicious package within the build chroot. This issue affects pc-kernel versions prior to and including 2019-07-16	8.4	More Details
CVE-2018-21070	An issue was discovered on Samsung mobile devices with N(7.x), O(8.0) devices (MSM8998 or SDM845 chipsets) software. An attacker can bypass Secure Boot and obtain root access because of a missing Bootloader integrity check. The Samsung ID is SVE-2018-11552 (May 2018).	8.4	More Details
CVE-2018-21082	An issue was discovered on Samsung mobile devices with N(7.x) software. Dex Station allows App Pinning bypass and lock-screen bypass via the "Use screen lock type to unpin" option. The Samsung ID is SVE-2017-11106 (February 2018).	8.4	More Details
CVE-2020-7800	The Synergy Systems & Solutions (SSS) HUSKY RTU 6049-E70, with firmware Versions 5.0 and prior, has an Improper Check for Unusual or Exceptional Conditions (CWE-754) vulnerability. The affected product is vulnerable to specially crafted TCP packets, which can cause the device to shut down or reboot and lose configuration settings. This is a different issue than CVE-2019-16879, CVE-2019-20045, CVE-2019-20046, CVE-2020-7801, and CVE-2020-7802.	8.2	More Details
CVE-2020-5550	Session fixation vulnerability in EasyBlocks IPv6 Ver. 2.0.1 and earlier, and Enterprise Ver. 2.0.1 and earlier allows remote attackers to impersonate a registered user and log in the management console, that may result in information alteration/disclosure via unspecified vectors.	8.1	More Details
CVE-2020-1992	A format string vulnerability in the Varrcvr daemon of PAN-OS on PA-7000 Series devices with a Log Forwarding Card (LFC) allows remote attackers to crash the daemon creating a denial of service condition or potentially execute code with root privileges. This issue affects Palo Alto Networks PAN-OS 9.0 versions before 9.0.7; PAN-OS 9.1 versions before 9.1.2 on PA-7000 Series devices with an LFC installed and configured. This issue requires WildFire services to be configured and enabled. This issue does not affect PAN-OS 8.1 and earlier releases. This issue does not affect any other PA Series firewalls.	8.1	More Details
CVE-2018-21086	An issue was discovered on Samsung mobile devices with L(5.x), M(6.0), and N(7.x) software. There is a race condition with a resultant double free in vnswap_init_backing_storage. The Samsung ID is SVE-2017-11177 (February 2018).	8.1	More Details
CVE-2018-21085	An issue was discovered on Samsung mobile devices with L(5.x), M(6.0), and N(7.x) software. There is a race condition with a resultant use-after-free in vnswap_deinit_backing_storage. The Samsung ID is SVE-2017-11176 (February 2018).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21040	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos 9810 chipsets) software. There is a race condition with a resultant use-after-free in the g2d driver. The Samsung ID is SVE-2018-12959 (December 2018).	8.1	More Details
CVE-2020-5330	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this vulnerability to retrieve sensitive data by sending a specially crafted request to the affected endpoints.	8.1	More Details
CVE-2018-21084	An issue was discovered on Samsung mobile devices with L(5.1), M(6.0), and N(7.x) software. There is a race condition with a resultant read-after-free issue in get_kek. The Samsung ID is SVE-2017-11174 (February 2018).	8.1	More Details
CVE-2020-11002	dropwizard-validation before versions 2.0.3 and 1.3.21 has a remote code execution vulnerability. A server-side template injection was identified in the self-validating feature enabling attackers to inject arbitrary Java EL expressions, leading to Remote Code Execution (RCE) vulnerability. If you are using a self-validating bean an upgrade to Dropwizard 1.3.21/2.0.3 or later is strongly recommended. The changes introduced in Dropwizard 1.3.19 and 2.0.2 for CVE-2020-5245 unfortunately did not fix the underlying issue completely. The issue has been fixed in dropwizard-validation 1.3.21 and 2.0.3 or later. We strongly recommend upgrading to one of these versions.	8.0	More Details
CVE-2020-1895	A large heap overflow could occur in Instagram for Android when attempting to upload an image with specially crafted dimensions. This affects versions prior to 128.0.0.26.128.	7.8	More Details
CVE-2020-10642	In Rockwell Automation RSLinx Classic versions 4.11.00 and prior, an authenticated local attacker could modify a registry key, which could lead to the execution of malicious code using system privileges when opening RSLinx Classic.	7.8	More Details
CVE-2020-1985	Incorrect Default Permissions on C:\Programdata\Secdo\Logs folder in Secdo allows local authenticated users to overwrite system files and gain escalated privileges. This issue affects all versions Secdo for Windows.	7.8	More Details
CVE-2020-1885	Writing to an unprivileged file from a privileged OVRRedir.exe process in Oculus Desktop before 1.44.0.32849 on Windows allows local users to write to arbitrary files and consequently gain privileges via vectors involving a hard link to a log file.	7.8	More Details
CVE-2020-10384	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.6.1. There is a local privilege escalation from the www-data account to the root account.	7.8	More Details
CVE-2020-11725	snd_ctl_elem_add in sound/core/control.c in the Linux kernel through 5.6.3 has a count=info->owner line, which later affects a private_size*count multiplication for unspecified "interesting side effects." NOTE: kernel engineers dispute this finding, because it could be relevant only if new callers were added that were unfamiliar with the misuse of the info->owner field to represent data unrelated to the "owner" concept. The existing callers, SNDRV_CTL_IOCTL_ELEM_ADD and SNDRV_CTL_IOCTL_ELEM_REPLACE, have been designed to misuse the info->owner field in a safe way	7.8	More Details
CVE-2020-10551	QQBrowser before 10.5.3870.400 installs a Windows service TsService.exe. This file is writable by anyone belonging to the NT AUTHORITY\Authenticated Users group, which includes all local and remote users. This can be abused by local attackers to escalate privileges to NT AUTHORITY\SYSTEM by writing a malicious executable to the location of TsService.	7.8	More Details
CVE-2020-1984	Secdo tries to execute a script at a hardcoded path if present, which allows a local authenticated user with 'create folders or append data' access to the root of the OS disk (C:\) to gain system privileges if the path does not already exist or is writable. This issue affects all versions of Secdo for Windows.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11739	An issue was discovered in Xen through 4.13.x, allowing guest OS users to cause a denial of service or possibly gain privileges because of missing memory barriers in read-write unlock paths. The read-write unlock paths don't contain a memory barrier. On Arm, this means a processor is allowed to re-order the memory access with the preceding ones. In other words, the unlock may be seen by another processor before all the memory accesses within the "critical" section. As a consequence, it may be possible to have a writer executing a critical section at the same time as readers or another writer. In other words, many of the assumptions (e.g., a variable cannot be modified after a check) in the critical sections are not safe anymore. The read-write locks are used in hypercalls (such as grant-table ones), so a malicious guest could exploit the race. For instance, there is a small window where Xen can leak memory if XENMAPSPACE_grant_table is used concurrently. A malicious guest may be able to leak memory, or cause a hypervisor crash resulting in a Denial of Service (DoS). Information leak and privilege escalation cannot be excluded.	7.8	More Details
CVE-2019-14326	An issue was discovered in AndyOS Andy versions up to 46.11.113. By default, it starts telnet and ssh (ports 22 and 23) with root privileges in the emulated Android system. This can be exploited by remote attackers to gain full access to the device, or by malicious apps installed inside the emulator to perform privilege escalation from a normal user to root (unlike with standard methods of getting root privileges on Android - e.g., the SuperSu program - the user is not asked for consent). There is no authentication performed - access to a root shell is given upon a successful connection. NOTE: although this was originally published with a slightly different CVE ID number, the correct ID for this Andy vulnerability has always been CVE-2019-14326.	7.8	More Details
CVE-2020-1991	An insecure temporary file vulnerability in Palo Alto Networks Traps allows a local authenticated Windows user to escalate privileges or overwrite system files. This issue affects Palo Alto Networks Traps 5.0 versions before 5.0.8; 6.1 versions before 6.1.4 on Windows. This issue does not affect Cortex XDR 7.0. This issue does not affect Traps for Linux or MacOS.	7.8	More Details
CVE-2020-10646	Fuji Electric V-Server Lite all versions prior to 4.0.9.0 contains a heap based buffer overflow. The buffer allocated to read data, when parsing VPR files, is too small.	7.8	More Details
CVE-2020-11738	The Snap Creek Duplicator plugin before 1.3.28 for WordPress (and Duplicator Pro before 3.8.7.1) allows Directory Traversal via ../ in the file parameter to duplicator_download or duplicator_init.	7.5	More Details
CVE-2019-20637	An issue was discovered in Varnish Cache before 6.0.5 LTS, 6.1.x and 6.2.x before 6.2.2, and 6.3.x before 6.3.1. It does not clear a pointer between the handling of one client request and the next request within the same connection. This sometimes causes information to be disclosed from the connection workspace, such as data structures associated with previous requests within this connection or VCL-related temporary headers.	7.5	More Details
CVE-2020-11655	SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the AggInfo object's initialization is mishandled.	7.5	More Details
CVE-2020-8826	As of v1.5.0, the Argo web interface authentication system issued immutable tokens. Authentication tokens, once issued, were usable forever without expiration—there was no refresh or forced re-authentication.	7.5	More Details
CVE-2020-10617	There are multiple ways an unauthenticated attacker could perform SQL injection on WebAccess/NMS (versions prior to 3.0.2) to gain access to sensitive information.	7.5	More Details
CVE-2020-8827	As of v1.5.0, the Argo API does not implement anti-automation measures such as rate limiting, account lockouts, or other anti-bruteforce measures. Attackers can submit an unlimited number of authentication attempts without consequence.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1639	When an attacker sends a specific crafted Ethernet Operation, Administration, and Maintenance (Ethernet OAM) packet to a target device, it may improperly handle the incoming malformed data and fail to sanitize this incoming data resulting in an overflow condition. This overflow condition in Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) condition by coring the CFM daemon. Continued receipt of these packets may cause an extended Denial of Service condition. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S15; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 14.1X50 versions prior to 14.1X50-D145; 14.1X53 versions prior to 14.1X53-D47; 15.1 versions prior to 15.1R2; 15.1X49 versions prior to 15.1X49-D170 on SRX Series; 15.1X53 versions prior to 15.1X53-D67.	7.5	More Details
CVE-2020-1617	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources.	7.5	More Details
CVE-2020-11557	An issue was discovered in Castle Rock SNMPc Online 12.10.10 before 2020-01-28. It includes the username and password values in cleartext within each request's cookie value.	7.5	More Details
CVE-2020-11555	An issue was discovered in Castle Rock SNMPc Online 12.10.10 before 2020-01-28. It allows remote attackers to obtain sensitive credential information from backup files.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1638	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO.	7.5	More Details
CVE-2020-1634	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions prior to 12.3X48-D95 on High-End SRX Series. This issue does not affect Branch SRX Series devices.	7.5	More Details
CVE-2020-11554	An issue was discovered in Castle Rock SNMPc Online 12.10.10 before 2020-01-28. It allows remote attackers to obtain sensitive information via info.php4.	7.5	More Details
CVE-2020-1626	A vulnerability in Juniper Networks Junos OS Evolved may allow an attacker to cause a Denial of Service (DoS) by sending a high rate of specific packets to the device, resulting in a pfemand process crash. The pfemand process is responsible for packet forwarding on the device. By continuously sending the packet flood, an attacker can repeatedly crash the pfemand process causing a sustained Denial of Service. This issue can only be triggered by traffic sent to the device. Transit traffic does not cause this issue. This issue affects all version of Junos OS Evolved prior to 19.1R1-EVO.	7.5	More Details
CVE-2020-1627	A vulnerability in Juniper Networks Junos OS on vMX and MX150 devices may allow an attacker to cause a Denial of Service (DoS) by sending specific packets requiring special processing in microcode that the flow cache can't handle, causing the riot forwarding daemon to crash. By continuously sending the same specific packets, an attacker can repeatedly crash the riot process causing a sustained Denial of Service. Flow cache is specific to vMX based products and the MX150, and is enabled by default in performance mode. This issue can only be triggered by traffic destined to the device. Transit traffic will not cause the riot daemon to crash. When the issue occurs, a core dump and riot log file entry are generated. For example: /var/crash/core.J-UKERN.mpc0.1557255993.3864.gz /home/pfe/RIOT logs: fpc0 riot[1888]: PANIC in lu_reorder_send_packet_postproc(): fpc0 riot[6655]: PANIC in lu_reorder_send_packet_postproc(): This issue affects Juniper Networks Junos OS: 18.1 versions prior to 18.1R3 on vMX and MX150; 18.2 versions prior to 18.2R3 on vMX and MX150; 18.2X75 versions prior to 18.2X75-D60 on vMX and MX150; 18.3 versions prior to 18.3R3 on vMX and MX150; 18.4 versions prior to 18.4R2 on vMX and MX150; 19.1 versions prior to 19.1R2 on vMX and MX150. This issue does not affect Junos OS versions prior to 18.1R1.	7.5	More Details
CVE-2020-10366	LogicalDoc before 8.3.3 allows /servlet.gupld Directory Traversal, a different vulnerability than CVE-2020-9423 and CVE-2020-10365.	7.5	More Details
CVE-2020-11650	An issue was discovered in iXsystems FreeNAS (and TrueNAS) 11.2 before 11.2-u8 and 11.3 before 11.3-U1. It allows a denial of service. The login authentication component has no limits on the length of an authentication message or the rate at which such messages are sent.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10976	GitLab EE/CE 8.17 to 12.9 is vulnerable to information leakage when querying a merge request widget.	7.5	More Details
CVE-2020-11605	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. There is sensitive information exposure from dumpstate in NFC logs. The Samsung ID is SVE-2019-16359 (April 2020).	7.5	More Details
CVE-2020-11732	The Media Library Assistant plugin before 2.82 for Wordpress suffers from a Local File Inclusion vulnerability in mla_gallery link=download.	7.5	More Details
CVE-2020-11724	An issue was discovered in OpenResty before 1.15.8.4. ngx_http_lua_subrequest.c allows HTTP request smuggling, as demonstrated by the ngx.location.capture API.	7.5	More Details
CVE-2020-11713	wolfSSL 4.3.0 has mulmod code in wc_ecc_mulmod_ex in ecc.c that does not properly resist timing side-channel attacks.	7.5	More Details
CVE-2020-11709	cpp-httplib through 0.5.8 does not filter \r\n in parameters passed into the set_redirect and set_header functions, which creates possibilities for CRLF injection and HTTP response splitting in some specific contexts.	7.5	More Details
CVE-2017-18643	An issue was discovered on Samsung mobile devices with M(6.x) and N(7.x) software. There is information disclosure of the kbase_context address of a GPU memory node. The Samsung ID is SVE-2017-8907 (December 2017).	7.5	More Details
CVE-2018-21091	An issue was discovered on Samsung mobile devices with M(6.x) and N(7.x) software. Telecom has a System Crash via abnormal exception handling. The Samsung ID is SVE-2017-10906 (January 2018).	7.5	More Details
CVE-2020-11703	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. /ajax/GetInheritedProperties allows HTTP Response Splitting via the language parameter.	7.5	More Details
CVE-2020-11694	In JetBrains PyCharm 2019.2.5 and 2019.3 on Windows, Apple Notarization Service credentials were included. This is fixed in 2019.2.6 and 2019.3.3.	7.5	More Details
CVE-2020-11647	In Wireshark 3.2.0 to 3.2.2, 3.0.0 to 3.0.9, and 2.6.0 to 2.6.15, the BACapp dissector could crash. This was addressed in epan/dissectors/packet-bacapp.c by limiting the amount of recursion.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19301	A vulnerability has been identified in SCALANCE X200-4P IRT, SCALANCE X201-3P IRT, SCALANCE X201-3P IRT PRO, SCALANCE X202-2IRT, SCALANCE X202-2P IRT, SCALANCE X202-2P IRT PRO, SCALANCE X204-2, SCALANCE X204-2FM, SCALANCE X204-2LD, SCALANCE X204-2LD TS, SCALANCE X204-2TS, SCALANCE X204IRT, SCALANCE X204IRT PRO, SCALANCE X206-1, SCALANCE X206-1LD, SCALANCE X208, SCALANCE X208PRO, SCALANCE X212-2, SCALANCE X212-2LD, SCALANCE X216, SCALANCE X224, SCALANCE X302-7 EEC (230V, coated), SCALANCE X302-7 EEC (230V), SCALANCE X302-7 EEC (24V, coated), SCALANCE X302-7 EEC (24V), SCALANCE X302-7 EEC (2x 230V, coated), SCALANCE X302-7 EEC (2x 230V), SCALANCE X302-7 EEC (2x 24V, coated), SCALANCE X302-7 EEC (2x 24V), SCALANCE X304-2FE, SCALANCE X306-1LD FE, SCALANCE X307-2 EEC (230V, coated), SCALANCE X307-2 EEC (230V), SCALANCE X307-2 EEC (24V, coated), SCALANCE X307-2 EEC (24V), SCALANCE X307-2 EEC (2x 230V, coated), SCALANCE X307-2 EEC (2x 230V), SCALANCE X307-2 EEC (2x 24V, coated), SCALANCE X307-2 EEC (2x 24V), SCALANCE X307-3, SCALANCE X307-3, SCALANCE X307-3LD, SCALANCE X307-3LD, SCALANCE X308-2, SCALANCE X308-2, SCALANCE X308-2LD, SCALANCE X308-2LD, SCALANCE X308-2LH, SCALANCE X308-2LH, SCALANCE X308-2LH+, SCALANCE X308-2LH+, SCALANCE X308-2M, SCALANCE X308-2M, SCALANCE X308-2M PoE, SCALANCE X308-2M PoE, SCALANCE X308-2M TS, SCALANCE X308-2M TS, SCALANCE X310, SCALANCE X310, SCALANCE X310FE, SCALANCE X310FE, SCALANCE X320-1 FE, SCALANCE X320-1-2LD FE, SCALANCE X408-2, SCALANCE XF201-3P IRT, SCALANCE XF202-2P IRT, SCALANCE XF204, SCALANCE XF204-2, SCALANCE XF204-2BA IRT, SCALANCE XF204IRT, SCALANCE XF206-1, SCALANCE XF208, SCALANCE XR324-12M (230V, ports on front), SCALANCE XR324-12M (230V, ports on front), SCALANCE XR324-12M (230V, ports on rear), SCALANCE XR324-12M (230V, ports on rear), SCALANCE XR324-12M (24V, ports on front), SCALANCE XR324-12M (24V, ports on front), SCALANCE XR324-12M (24V, ports on rear), SCALANCE XR324-12M (24V, ports on rear), SCALANCE XR324-12M TS (24V), SCALANCE XR324-12M TS (24V), SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front), SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front), SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear), SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear), SCALANCE XR324-4M EEC (24V, ports on front), SCALANCE XR324-4M EEC (24V, ports on front), SCALANCE XR324-4M EEC (24V, ports on rear), SCALANCE XR324-4M EEC (24V, ports on rear), SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front), SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front), SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear), SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear), SCALANCE XR324-4M EEC (2x 24V, ports on front), SCALANCE XR324-4M EEC (2x 24V, ports on front), SCALANCE XR324-4M EEC (2x 24V, ports on rear), SCALANCE XR324-4M EEC (2x 24V, ports on rear), SCALANCE XR324-4M PoE (230V, ports on front), SCALANCE XR324-4M PoE (230V, ports on rear), SCALANCE XR324-4M PoE (24V, ports on front), SCALANCE XR324-4M PoE (24V, ports on rear), SCALANCE XR324-4M PoE TS (24V, ports on front), SIMATIC CP 343-1 Advanced, SIMATIC CP 442-1 RNA, SIMATIC CP 443-1, SIMATIC CP 443-1, SIMATIC CP 443-1 Advanced, SIMATIC CP 443-1 RNA, SIMATIC RF180C, SIMATIC RF182C, SIPLUS NET CP 343-1 Advanced, SIPLUS NET CP 443-1, SIPLUS NET CP 443-1 Advanced, SIPLUS NET SCALANCE X308-2. The VxWorks-based Profinet TCP Stack can be forced to make very expensive calls for every incoming packet which can lead to a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19300	A vulnerability has been identified in Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200, Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P, KTK ATE530S, SIDOOR ATD430W, SIDOOR ATE530S COATED, SIDOOR ATE531S, SIMATIC ET 200AL IM 157-1 PN (6ES7157-1AB00-0AB0), SIMATIC ET 200MP IM 155-5 PN HF (6ES7155-5AA00-0AC0), SIMATIC ET 200pro IM 154-8 PN/DP CPU (6ES7154-8AB01-0AB0), SIMATIC ET 200pro IM 154-8F PN/DP CPU (6ES7154-8FB01-0AB0), SIMATIC ET 200pro IM 154-8FX PN/DP CPU (6ES7154-8FX00-0AB0), SIMATIC ET 200S IM 151-8 PN/DP CPU (6ES7151-8AB01-0AB0), SIMATIC ET 200S IM 151-8F PN/DP CPU (6ES7151-8FB01-0AB0), SIMATIC ET 200SP IM 155-6 MF HF (6ES7155-6MU00-0CN0), SIMATIC ET 200SP IM 155-6 PN HA (incl. SIPLUS variants), SIMATIC ET 200SP IM 155-6 PN HF (6ES7155-6AU00-0CN0), SIMATIC ET 200SP IM 155-6 PN/2 HF (6ES7155-6AU01-0CN0), SIMATIC ET 200SP IM 155-6 PN/3 HF (6ES7155-6AU30-0CN0), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants), SIMATIC ET200ecoPN, AI 8xRTD/TC, M12-L (6ES7144-6JF00-0BB0), SIMATIC ET200ecoPN, CM 4x IO-Link, M12-L (6ES7148-6JE00-0BB0), SIMATIC ET200ecoPN, CM 8x IO-Link, M12-L (6ES7148-6JG00-0BB0), SIMATIC ET200ecoPN, CM 8x IO-Link, M12-L (6ES7148-6JJ00-0BB0), SIMATIC ET200ecoPN, DI 16x24VDC, M12-L (6ES7141-6BH00-0BB0), SIMATIC ET200ecoPN, DI 8x24VDC, M12-L (6ES7141-6BG00-0BB0), SIMATIC ET200ecoPN, DIQ 16x24VDC/2A, M12-L (6ES7143-6BH00-0BB0), SIMATIC ET200ecoPN, DQ 8x24VDC/0,5A, M12-L (6ES7142-6BG00-0BB0), SIMATIC ET200ecoPN, DQ 8x24VDC/2A, M12-L (6ES7142-6BR00-0BB0), SIMATIC MICRO-DRIVE PDC, SIMATIC PN/MF Coupler (6ES7158-3MU10-0XA0), SIMATIC PN/PN Coupler (6ES7158-3AD10-0XA0), SIMATIC S7-1200 CPU family (incl. SIPLUS variants), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants), SIMATIC S7-1500 Software Controller, SIMATIC S7-300 CPU 314C-2 PN/DP (6ES7314-6EH04-0AB0), SIMATIC S7-300 CPU 315-2 PN/DP (6ES7315-2EH14-0AB0), SIMATIC S7-300 CPU 315F-2 PN/DP (6ES7315-2FJ14-0AB0), SIMATIC S7-300 CPU 315T-3 PN/DP (6ES7315-7TJ10-0AB0), SIMATIC S7-300 CPU 317-2 PN/DP (6ES7317-2EK14-0AB0), SIMATIC S7-300 CPU 317F-2 PN/DP (6ES7317-2FK14-0AB0), SIMATIC S7-300 CPU 317T-3 PN/DP (6ES7317-7TK10-0AB0), SIMATIC S7-300 CPU 317TF-3 PN/DP (6ES7317-7UL10-0AB0), SIMATIC S7-300 CPU 319-3 PN/DP (6ES7318-3EL01-0AB0), SIMATIC S7-300 CPU 319F-3 PN/DP (6ES7318-3FL01-0AB0), SIMATIC S7-400 H V6 and below CPU family (incl. SIPLUS variants), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants), SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants), SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants), SIMATIC TDC CP51M1, SIMATIC TDC CPU555, SIMATIC WinAC RTX 2010 (6ES7671-0RC08-0YA0), SIMATIC WinAC RTX F 2010 (6ES7671-1RC08-0YA0), SINAMICS S/G Control Unit w. PROFINET, SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-2AC0), SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-7AC0), SIPLUS ET 200MP IM 155-5 PN HF T1 RAIL (6AG2155-5AA00-1AC0), SIPLUS ET 200S IM 151-8 PN/DP CPU (6AG1151-8AB01-7AB0), SIPLUS ET 200S IM 151-8F PN/DP CPU (6AG1151-8FB01-2AB0), SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU00-2CN0), SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU00-4CN0), SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU01-2CN0), SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU01-7CN0), SIPLUS ET 200SP IM 155-6 PN HF T1 RAIL (6AG2155-6AU00-1CN0), SIPLUS ET 200SP IM 155-6 PN HF T1 RAIL (6AG2155-6AU01-1CN0), SIPLUS ET 200SP IM 155-6 PN HF TX RAIL (6AG2155-6AU01-4CN0), SIPLUS NET PN/PN Coupler (6AG2158-3AD10-4XA0), SIPLUS S7-300 CPU 314C-2 PN/DP (6AG1314-6EH04-7AB0), SIPLUS S7-300 CPU 315-2 PN/DP (6AG1315-2EH14-7AB0), SIPLUS S7-300 CPU 315F-2 PN/DP (6AG1315-2FJ14-2AB0), SIPLUS S7-300 CPU 317-2 PN/DP (6AG1317-2EK14-7AB0), SIPLUS S7-300 CPU 317F-2 PN/DP (6AG1317-2FK14-2AB0). The Interniche-based TCP Stack can be forced to make very expensive calls for every incoming packet which can lead to a denial of service.	7.5	More Details
CVE-2020-6237	Under certain conditions, SAP Business Objects Business Intelligence Platform, version 4.1, 4.2, dswsbobje web application allows an attacker to access information which would otherwise be restricted, leading to Information Disclosure.	7.5	More Details
CVE-2018-21083	An issue was discovered on Samsung mobile devices with M(6.0), N(7.x), and O(8.0) (Exynos or Qualcomm chipsets) software. There is information disclosure (of a kernel address) via trustonic_tee. The Samsung ID is SVE-2017-11175 (February 2018).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10629	WebAccess/NMS (versions prior to 3.0.2) does not sanitize XML input. Specially crafted XML input could allow an attacker to read sensitive files.	7.5	More Details
CVE-2018-21088	An issue was discovered on Samsung mobile devices with N(7.x) software. An attacker can cause a reboot because InputMethodManagerService has an unprotected system service. The Samsung ID is SVE-2017-9995 (January 2018).	7.5	More Details
CVE-2015-9547	An issue was discovered on Samsung mobile devices with JBP(4.3) and KK(4.4.2) software. Because the READ_LOGS permission is mishandled, sensitive information is disclosed in a world-readable copy of the log file if the error message is "Unhandled exception in Dalvik VM," "Application not responding ANR event," or "Crash on an application's native code." The Samsung ID is SVE-2015-2885 (October 2015).	7.5	More Details
CVE-2018-6402	Ecobee Ecobee4 4.2.0.171 devices can be forced to deauthenticate and connect to an unencrypted Wi-Fi network with the same SSID, even if the device settings specify use of encryption such as WPA2, as long as the competing network has a stronger signal. An attacker must be able to set up a nearby SSID, similar to an "Evil Twin" attack.	7.5	More Details
CVE-2018-21041	An issue was discovered on Samsung mobile devices with O(8.x) software. Access to Gallery in the Secure Folder can occur without authentication. The Samsung ID is SVE-2018-13057 (December 2018).	7.5	More Details
CVE-2018-21079	An issue was discovered on Samsung mobile devices with L(5.x), M(6.0), N(7.x), and O(8.0) software. There is a kernel pointer leak in the USB gadget driver. The Samsung ID is SVE-2017-10993 (March 2018).	7.5	More Details
CVE-2020-6228	SAP Business Client, versions 6.5, 7.0, does not perform necessary integrity checks which could be exploited by an attacker under certain conditions to modify the installer.	7.5	More Details
CVE-2020-6227	SAP Business Objects Business Intelligence Platform (CMS / Auditing issues), version 4.2, allows attacker to send specially crafted GIOP packets to several services due to Improper Input Validation, allowing to forge additional entries in GLF log files.	7.5	More Details
CVE-2018-21047	An issue was discovered on Samsung mobile devices with O(8.x) software. There is a Factory Reset Protection (FRP) bypass via the voice assistant because Internet access begins before the Setup Wizard finishes. The Samsung ID is SVE-2018-12894 (November 2018).	7.5	More Details
CVE-2018-21059	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. There is Clipboard content visibility in the locked state via the emergency contact picker. The Samsung ID is SVE-2018-11806 (September 2018).	7.5	More Details
CVE-2018-21060	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. There is a Keyboard learned words leak in the locked state via the emergency contact picker. The Samsung IDs are SVE-2018-11989, SVE-2018-11990 (September 2018).	7.5	More Details
CVE-2020-11653	An issue was discovered in Varnish Cache before 6.0.6 LTS, 6.1.x and 6.2.x before 6.2.3, and 6.3.x before 6.3.2. It occurs when communication with a TLS termination proxy uses PROXY version 2. There can be an assertion failure and daemon restart, which causes a performance loss.	7.5	More Details
CVE-2018-21039	An issue was discovered on Samsung mobile devices with N(7.0) software. With the Location permission for the compass feature in Quick Tools (aka QuickTools), an attacker can bypass the lockscreen. The Samsung ID is SVE-2018-12053 (December 2018).	7.5	More Details
CVE-2018-21078	An issue was discovered on Samsung mobile devices with M(6.0), N(7.x), and O(8.0) software. The Contacts application allows attackers to originate video calls because SS (Supplementary Service) and USSD (Unstructured Supplementary Service Data) codes are improperly secured. The Samsung ID is SVE-2018-11469 (April 2018).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21069	An issue was discovered on Samsung mobile devices with N(7.x) (MediaTek chipsets) software. There is information disclosure (of kernel stack memory) in a MediaTek driver. The Samsung ID is SVE-2018-11852 (July 2018).	7.5	More Details
CVE-2020-1633	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series.	7.4	More Details
CVE-2018-21071	An issue was discovered on Samsung mobile devices with M(6.0) software. Because of an unprotected intent, an attacker can read arbitrary files and emails, and take over an email account. The Samsung ID is SVE-2018-11633 (May 2018).	7.3	More Details
CVE-2020-8327	A privilege escalation vulnerability was reported in LenovoBatteryGaugePackage for Lenovo System Interface Foundation bundled in Lenovo Vantage prior to version 10.2003.10.0 that could allow an authenticated user to execute code with elevated privileges.	7.3	More Details
CVE-2020-8319	A privilege escalation vulnerability was reported in Lenovo System Interface Foundation prior to version 1.1.19.3 that could allow an authenticated user to execute code with elevated privileges.	7.3	More Details
CVE-2020-8318	A privilege escalation vulnerability was reported in the LenovoSystemUpdatePlugin for Lenovo System Interface Foundation prior to version that could allow an authenticated user to execute code with elevated privileges.	7.3	More Details
CVE-2020-6765	D-Link DSL-GS225 J1 AU_1.0.4 devices allow an admin to execute OS commands by placing shell metacharacters after a supported CLI command, as demonstrated by ping -c1 127.0.0.1; cat/etc/passwd. The CLI is reachable by TELNET.	7.2	More Details
CVE-2020-9499	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down.	7.2	More Details
CVE-2020-1990	A stack-based buffer overflow vulnerability in the management server component of PAN-OS allows an authenticated user to upload a corrupted PAN-OS configuration and potentially execute code with root privileges. This issue affects Palo Alto Networks PAN-OS 8.1 versions before 8.1.13; 9.0 versions before 9.0.7. This issue does not affect PAN-OS 7.1.	7.2	More Details
CVE-2020-11629	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. The External Command Certificate Validator, which allows administrators to upload external linters to validate certificates, is supposed to save uploaded test certificates to the server. An attacker who has gained access to the CA UI could exploit this to upload malicious scripts to the server. (Risks associated with this issue alone are negligible unless a malicious user already has gained access to the CA UI through other means, as a trusted user is already trusted to upload scripts by virtue of having access to the validator.)	7.2	More Details
CVE-2020-6230	SAP OrientDB, version 3.0, allows an authenticated attacker with script execute/write permissions to inject code that can be executed by the application and lead to Code Injection. An attacker could thereby control the behavior of the application.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6234	SAP Host Agent, version 7.21, allows an attacker with admin privileges to use the operation framework to gain root privileges over the underlying operating system, leading to Privilege Escalation.	7.2	More Details
CVE-2020-6236	SAP Landscape Management, version 3.0, and SAP Adaptive Extensions, version 1.0, allows an attacker with admin_group privileges to change ownership and permissions (including S-user ID bit s-bit) of arbitrary files remotely. This results in the possibility to execute these files as root user from a non-root context, leading to Privilege Escalation.	7.2	More Details
CVE-2020-1637	A vulnerability in Juniper Networks SRX Series device configured as a Junos OS Enforcer device may allow a user to access network resources that are not permitted by a UAC policy. This issue might occur when the IP address range configured in the Infranet Controller (IC) is configured as an IP address range instead of an IP address/netmask. See the Workaround section for more detail. The Junos OS Enforcer CLI settings are disabled by default. This issue affects Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D100; 15.1X49 versions prior to 15.1X49-D210; 17.3 versions prior to 17.3R2-S5, 17.3R3-S8; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R3-S2; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2-S1, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2.	7.2	More Details
CVE-2020-11668	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.	7.1	More Details
CVE-2020-1989	An incorrect privilege assignment vulnerability when writing application-specific files in the Palo Alto Networks Global Protect Agent for Linux on ARM platform allows a local authenticated user to gain root privileges on the system. This issue affects Palo Alto Networks Global Protect Agent for Linux 5.0 versions before 5.0.8; 5.1 versions before 5.1.1.	7.0	More Details
CVE-2018-21061	An issue was discovered on Samsung mobile devices with N(7.1) and O(8.x) software. A fake charger can execute critical functions in the locked state. The Samsung ID is SVE-2016-6341 (August 2018).	6.8	More Details
CVE-2020-10262	An issue was discovered on XIAOMI XIAOAI speaker Pro LX06 1.58.10. Attackers can activate the failsafe mode during the boot process, and use the mi_console command cascaded by the SN code shown on the product to get the root shell password, and then the attacker can (i) read Wi-Fi SSID or password, (ii) read the dialogue text files between users and XIAOMI XIAOAI speaker Pro LX06, (iii) use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, (iv) eavesdrop on users and record what XIAOMI XIAOAI speaker Pro LX06 hears, (v) modify system files, (vi) use commands to send any IR code through IR emitter on XIAOMI XIAOAI Speaker Pro (LX06), (vii) stop voice assistant service, (viii) enable the XIAOMI XIAOAI Speaker Pro's SSH or TELNET service as a backdoor, (IX) tamper with the router configuration of the router in the local area networks.	6.8	More Details
CVE-2020-10263	An issue was discovered on XIAOMI XIAOAI speaker Pro LX06 1.52.4. Attackers can get root shell by accessing the UART interface and then they can (i) read Wi-Fi SSID or password, (ii) read the dialogue text files between users and XIAOMI XIAOAI speaker Pro LX06, (iii) use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, (iv) eavesdrop on users and record what XIAOMI XIAOAI speaker Pro LX06 hears, (v) modify system files, (vi) use commands to send any IR code through IR emitter on XIAOMI XIAOAI Speaker Pro LX06, (vii) stop voice assistant service, (viii) enable the XIAOMI XIAOAI Speaker Pro' SSH or TELNET service as a backdoor, (IX) tamper with the router configuration of the router in the local area networks.	6.8	More Details
CVE-2019-20636	In the Linux kernel before 5.4.12, drivers/input/input.c has out-of-bounds writes via a crafted keycode table, as demonstrated by input_set_keycode, aka CID-cb222aed03d7.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5406	VMware Tanzu Application Service for VMs, 2.6.x versions prior to 2.6.18, 2.7.x versions prior to 2.7.11, and 2.8.x versions prior to 2.8.5, includes a version of PCF Autoscaling that writes database connection properties to its log, including database username and password. A malicious user with access to those logs may gain unauthorized access to the database being used by Autoscaling.	6.5	More Details
CVE-2019-18375	The ASG and ProxySG management consoles are susceptible to a session hijacking vulnerability. A remote attacker, with access to the appliance management interface, can hijack the session of a currently logged-in user and access the management console.	6.5	More Details
CVE-2020-8834	KVM in the Linux kernel on Power8 processors has a conflicting use of HSTATE_HOST_R1 to store r1 state in kvmppc_hv_entry plus in kvmppc_{save,restore}_tm, leading to a stack corruption. Because of this, an attacker with the ability run code in kernel space of a guest VM can cause the host kernel to panic. There were two commits that, according to the reporter, introduced the vulnerability: f024ee098476 ("KVM: PPC: Book3S HV: Pull out TM state save/restore into separate procedures") 87a11bb6a7f7 ("KVM: PPC: Book3S HV: Work around XER[SO] bug in fake suspend mode") The former landed in 4.8, the latter in 4.17. This was fixed without realizing the impact in 4.18 with the following three commits, though it's believed the first is the only strictly necessary commit: 6f597c6b63b6 ("KVM: PPC: Book3S PR: Add guest MSR parameter for kvmppc_save_tm()/kvmppc_restore_tm()") 7b0e827c6970 ("KVM: PPC: Book3S HV: Factor fake-suspend handling out of kvmppc_save/restore_tm") 009c872a8bc4 ("KVM: PPC: Book3S PR: Move kvmppc_save_tm/kvmppc_restore_tm to separate file")	6.5	More Details
CVE-2020-6446	Insufficient policy enforcement in trusted types in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass content security policy via a crafted HTML page.	6.5	More Details
CVE-2018-21034	In Argo versions prior to v1.5.0-rc1, it was possible for authenticated Argo users to submit API calls to retrieve secrets and other manifests which were stored within git.	6.5	More Details
CVE-2020-5736	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device.	6.5	More Details
CVE-2020-4151	IBM QRadar SIEM 7.3.0 through 7.3.3 could allow an authenticated attacker to perform unauthorized actions due to improper input validation. IBM X-Force ID: 174201.	6.5	More Details
CVE-2020-10623	Multiple vulnerabilities could allow an attacker with low privileges to perform SQL injection on WebAccess/NMS (versions prior to 3.0.2) to gain access to sensitive information.	6.5	More Details
CVE-2020-6456	Insufficient validation of untrusted input in clipboard in Google Chrome prior to 81.0.4044.92 allowed a local attacker to bypass site isolation via crafted clipboard contents.	6.5	More Details
CVE-2020-11721	load_png in loader.c in libsixel.a in libsixel 1.8.6 has an uninitialized pointer leading to an invalid call to free, which can cause a denial of service.	6.5	More Details
CVE-2020-6445	Insufficient policy enforcement in trusted types in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass content security policy via a crafted HTML page.	6.5	More Details
CVE-2020-11631	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. An error state can be generated in the CA UI by a malicious user. This, in turn, allows exploitation of other bugs. This follow-on exploitation can lead to privilege escalation and remote code execution. (This is exploitable only when at least one accessible port lacks a requirement for client certificate authentication. These ports are 8442 or 8080 in a standard installation.)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1625	The kernel memory usage represented as "temp" via 'show system virtual-memory' may constantly increase when Integrated Routing and Bridging (IRB) is configured with multiple underlay physical interfaces, and one interface flaps. This memory leak can affect running daemons (processes), leading to an extended Denial of Service (DoS) condition. Usage of "temp" virtual memory, shown here by a constantly increasing value of outstanding Requests, can be monitored by executing the 'show system virtual-memory' command as shown below: user@junos> show system virtual-memory |match "fpc|type|temp" fpc0: ---------- Type InUse MemUse HighUse Requests Size(s) temp 2023 431K - 10551 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 fpc1: ---------- Type InUse MemUse HighUse Requests Size(s) temp 2020 431K - 6460 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 user@junos> show system virtual-memory |match "fpc|type|temp" fpc0: ---------- Type InUse MemUse HighUse Requests Size(s) temp 2023 431K - 16101 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 fpc1: ---------- Type InUse MemUse HighUse Requests Size(s) temp 2020 431K - 6665 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 user@junos> show system virtual-memory |match "fpc|type|temp" fpc0: ---------- Type InUse MemUse HighUse Requests Size(s) temp 2023 431K - 21867 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 fpc1: ---------- Type InUse MemUse HighUse Requests Size(s) temp 2020 431K - 6858 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S6; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.2X75 versions prior to 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S5, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R2-S5, 18.2R3; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60; 18.3 versions prior to 18.3R1-S5, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S2, 18.4R3; 19.1 versions prior to 19.1R1-S3, 19.1R2; 19.2 versions prior to 19.2R1-S3, 19.2R2. This issue does not affect Juniper Networks Junos OS 12.3 and 15.1.	6.5	More Details
CVE-2018-21092	An issue was discovered on Samsung mobile devices with M(6.x) and N(7.x) software. A crafted AT command may be sent by the DeviceTest application via an NFC tag. The Samsung ID is SVE-2017-10885 (January 2018).	6.5	More Details
CVE-2020-1759	A vulnerability was found in Red Hat Ceph Storage 4 and Red Hat Openshift Container Storage 4.2 where, A nonce reuse vulnerability was discovered in the secure mode of the messenger v2 protocol, which can allow an attacker to forge auth tags and potentially manipulate the data by leveraging the reuse of a nonce in a session. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks.	6.4	More Details
CVE-2020-7922	X.509 certificates generated by the MongoDB Enterprise Kubernetes Operator may allow an attacker with access to the Kubernetes cluster improper access to MongoDB instances. Customers who do not use X.509 authentication, and those who do not use the Operator to generate their X.509 certificates are unaffected. This issue affects MongoDB Enterprise Kubernetes Operator version 1.0, MongoDB Enterprise Kubernetes Operator version 1.1, MongoDB Enterprise Kubernetes Operator version 1.2 versions prior to 1.2.4, MongoDB Enterprise Kubernetes Operator version 1.3 versions prior to 1.3.1, 1.2, 1.4 versions prior to 1.4.4.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1618	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command “request system zeroize”; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3.	6.3	More Details
CVE-2020-6444	Uninitialized use in WebRTC in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	6.3	More Details
CVE-2018-21048	An issue was discovered on Samsung mobile devices with O(8.x) software. There is a Notification leak on a locked device in Standalone Dex mode. The Samsung ID is SVE-2018-12925 (November 2018).	6.2	More Details
CVE-2018-21068	An issue was discovered on Samsung mobile devices with O(8.0) software. Execution of an application in a locked Secure Folder can occur without a password via a split screen. The Samsung ID is SVE-2018-11669 (July 2018).	6.2	More Details
CVE-2020-6224	SAP NetWeaver AS Java (HTTP Service), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker with administrator privileges to access user sensitive data such as passwords in trace files, when the user logs in and sends request with login credentials, leading to Information Disclosure.	6.2	More Details
CVE-2018-21045	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. There is Clipboard access in the lockscreen state via a copy-and-paste action. The Samsung ID is SVE-2018-13381 (December 2018).	6.2	More Details
CVE-2020-11626	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. Two Cross Side Scripting (XSS) vulnerabilities have been found in the Public Web and the Certificate/CRL download servlets.	6.1	More Details
CVE-2020-11704	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. The Admin Web Interface has Multiple Stored and Reflected XSS. GetInheritedProperties is Reflected via the groups parameter. GetUserInfo is Reflected via POST data. SetUserInfo is Stored via the general parameter.	6.1	More Details
CVE-2020-11731	The Media Library Assistant plugin before 2.82 for Wordpress suffers from multiple XSS vulnerabilities in all Settings/Media Library Assistant tabs, which allow remote authenticated users to execute arbitrary JavaScript.	6.1	More Details
CVE-2020-8430	Stormshield Network Security 310 3.7.10 devices have an auth/lang.html?rurl= Open Redirect vulnerability on the captive portal. For example, the attacker can use rurl=//example.com instead of rurl=https://example.com in the query string.	6.1	More Details
CVE-2020-10633	A non-persistent XSS (cross-site scripting) vulnerability exists in eWON Flexy and Cosy (all firmware versions prior to 14.1s0). An attacker could send a specially crafted URL to initiate a password change for the device. The target must introduce the credentials to the gateway before the attack can be successful.	6.1	More Details
CVE-2020-11712	Open Upload through 0.4.3 allows XSS via index.php?action=u and the filename field.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6216	SAP Business Objects Business Intelligence Platform (BI Launchpad), version 4.2, does not sufficiently encode user-controlled inputs, resulting in reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2020-6229	SAP NetWeaver AS ABAP (Business Server Pages application CRM_BSP_FRAME), versions 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 75A, 75B, 75C, 75D, 75E, does not sufficiently encode user controlled inputs, resulting in reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2020-6223	The open document of SAP Business Objects Business Intelligence Platform, versions 4.1, 4.2, allows an attacker to modify certain error pages to include malicious content. This can misdirect a user who is tricked into accessing these error pages rendered by the application, leading to Content Spoofing.	6.1	More Details
CVE-2020-11702	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. The User Web Interface has Multiple Stored and Reflected XSS issues. Collaborate is Reflected via the filename parameter. Collaborate is Stored via the displayname parameter. Deletemultiple is Reflected via the files parameter. Share is Reflected via the target parameter. Share is Stored via the displayname parameter. Waitedit is Reflected via the Host header.	6.1	More Details
CVE-2020-7574	A vulnerability has been identified in Climatix POL908 (BACnet/IP module) (All versions), Climatix POL909 (AWM module) (All versions < V11.32). A persistent cross-site scripting (XSS) vulnerability exists in the "Server Config" web interface of the affected devices that could allow an attacker to inject arbitrary JavaScript code. The code could be potentially executed later by another (possibly privileged) user. The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no system privileges. An attacker could use the vulnerability to compromise the confidentiality and integrity of other users' web session.	6.1	More Details
CVE-2020-6217	SAP NetWeaver AS ABAP Business Server Pages Test Application IT00, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, does not sufficiently encode user-controlled inputs, resulting in reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2020-6215	SAP NetWeaver AS ABAP Business Server Pages Test Application IT00, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, allows an attacker to redirect users to a malicious site due to insufficient URL validation and steal credentials of the victim, leading to URL Redirection vulnerability.	6.1	More Details
CVE-2020-6211	SAP Business Objects Business Intelligence Platform (AdminTools), versions 4.1, 4.2, allows an attacker to redirect users to a malicious site due to insufficient URL validation and steal credentials of the victim, leading to URL Redirection vulnerability.	6.1	More Details
CVE-2020-11734	cgi-bin/go in CyberSolutions CyberMail 5 or later allows XSS via the ACTION parameter.	6.1	More Details
CVE-2020-7575	A vulnerability has been identified in Climatix POL908 (BACnet/IP module) (All versions), Climatix POL909 (AWM module) (All versions < V11.32). A persistent cross-site scripting (XSS) vulnerability exists in the web server access log page of the affected devices that could allow an attacker to inject arbitrary JavaScript code via specially crafted GET requests. The code could be potentially executed later by another (privileged) user. The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no system privileges. An attacker could use the vulnerability to compromise the confidentiality and integrity of other users' web sessions.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7958	An issue was discovered on OnePlus 7 Pro devices before 10.0.3.GM21BA. The firmware was found to contain functionality that allows a privileged user (root) in the Rich Execution Environment (REE) to obtain bitmap images from the fingerprint sensor because of Leftover Debug Code. The issue is that the Trusted Application (TA) supports an extended number of commands beyond what is needed to implement a fingerprint authentication system compatible with Android. An attacker who is in the position to send commands to the TA (for example, the root user) is able to send a sequence of these commands that will result in the TA sending a raw fingerprint image to the REE. This means that the Trusted Execution Environment (TEE) no longer protects identifiable fingerprint data from the REE.	6.0	More Details
CVE-2020-1619	A privilege escalation vulnerability in Juniper Networks QFX10K Series, EX9200 Series, MX Series, and PTX Series with Next-Generation Routing Engine (NG-RE), allows a local authenticated high privileged user to access the underlying WRL host. This issue only affects QFX10K Series with NG-RE, EX9200 Series with NG-RE, MX Series with NG-RE and PTX Series with NG-RE; which uses vmhost. This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S6; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S7, 17.4R3; 18.1 versions prior to 18.1R3-S4; 18.2 versions prior to 18.2R3; 18.2X75 versions prior to 18.2X75-D50; 18.3 versions prior to 18.3R2; 18.4 versions prior to 18.4R2. To identify whether the device has NG-RE with vmhost, customer can run the following command: > show vmhost status Compute cluster: rainier-re-cc Compute Node: rainier-re-cn, Online If the "show vmhost status" is not supported, then the device does not have NG-RE with vmhost.	6.0	More Details
CVE-2019-18376	A CSRF token disclosure vulnerability allows a remote attacker, with access to an authenticated Management Center (MC) user's web browser history or a network device that intercepts/logs traffic to MC, to obtain CSRF tokens and use them to perform CSRF attacks against MC.	5.9	More Details
CVE-2020-1629	A race condition vulnerability on Juniper Network Junos OS devices may cause the routing protocol daemon (RPD) process to crash and restart while processing a BGP NOTIFICATION message. This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S6; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3; 17.2 version 17.2R2 and later versions; 17.2X75 versions prior to 17.2X75-D105, 17.2X75-D110; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S7, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D410, 18.2X75-D420, 18.2X75-D50, 18.2X75-D60; 18.3 versions prior to 18.3R1-S5, 18.3R2-S2, 18.3R3; 18.4 versions prior to 18.4R2-S2, 18.4R3; 19.1 versions prior to 19.1R1-S2, 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. This issue does not affect Juniper Networks Junos OS prior to version 16.1R1.	5.9	More Details
CVE-2020-11001	In Wagtail before versions 2.8.1 and 2.7.2, a cross-site scripting (XSS) vulnerability exists on the page revision comparison view within the Wagtail admin interface. A user with a limited-permission editor account for the Wagtail admin could potentially craft a page revision history that, when viewed by a user with higher privileges, could perform actions with that user's credentials. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. Patched versions have been released as Wagtail 2.7.2 (for the LTS 2.7 branch) and Wagtail 2.8.1 (for the current 2.8 branch).	5.8	More Details
CVE-2019-7305	Information Exposure vulnerability in eXtplorer makes the /usr/ and /etc/extplorer/ system directories world-accessible over HTTP. Introduced in the Makefile patch file debian/patches/debian-changes-2.1.0b6+dfsg-1 or debian/patches/adds-a-makefile.patch, this can lead to data leakage, information disclosure and potentially remote code execution on the web server. This issue affects all versions of eXtplorer in Ubuntu and Debian	5.8	More Details
CVE-2020-2732	A flaw was discovered in the way that the KVM hypervisor handled instruction emulation for an L2 guest when nested virtualisation is enabled. Under some circumstances, an L2 guest may trick the L0 guest into accessing sensitive L1 resources that should be inaccessible to the L2 guest.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1978	TechSupport files generated on Palo Alto Networks VM Series firewalls for Microsoft Azure platform configured with high availability (HA) inadvertently collect Azure dashboard service account credentials. These credentials are equivalent to the credentials associated with the Contributor role in Azure. A user with the credentials will be able to manage all the Azure resources in the subscription except for granting access to other resources. These credentials do not allow login access to the VMs themselves. This issue affects VM Series Plugin versions before 1.0.9 for PAN-OS 9.0. This issue does not affect VM Series in non-HA configurations or on other cloud platforms. It does not affect hardware firewall appliances. Since becoming aware of the issue, Palo Alto Networks has safely deleted all the tech support files with the credentials. We now filter and remove these credentials from all TechSupport files sent to us. The TechSupport files uploaded to Palo Alto Networks systems were only accessible by authorized personnel with valid Palo Alto Networks credentials. We do not have any evidence of malicious access or use of these credentials.	5.8	More Details
CVE-2020-11000	GreenBrowser before version 1.2 has a vulnerability where apps that rely on URL Parsing to verify that a given URL is pointing to a trust server may be susceptible to many different ways to get URL parsing and verification wrong, which allows an attacker to circumvent the access control. This problem has been patched in version 1.2.	5.7	More Details
CVE-2020-11765	An issue was discovered in OpenEXR before 2.4.1. There is an off-by-one error in use of the ImfXdr.h read function by DwaCompressor::Classifier::Classifier, leading to an out-of-bounds read.	5.5	More Details
CVE-2020-1624	A local, authenticated user with shell can obtain the hashed values of login passwords and shared secrets via raw objmon configuration files. This issue affects all versions of Junos OS Evolved prior to 19.1R1.	5.5	More Details
CVE-2020-1623	A local, authenticated user with shell can view sensitive configuration information via the ev.ops configuration file. This issue affects all versions of Junos OS Evolved prior to 19.2R1.	5.5	More Details
CVE-2020-1622	A local, authenticated user with shell can obtain the hashed values of login passwords and shared secrets via the EvoSharedObjStore. This issue affects all versions of Junos OS Evolved prior to 19.1R1.	5.5	More Details
CVE-2020-1621	A local, authenticated user with shell can obtain the hashed values of login passwords via configd traces. This issue affects all versions of Junos OS Evolved prior to 19.3R1.	5.5	More Details
CVE-2020-1620	A local, authenticated user with shell can obtain the hashed values of login passwords via configd streamer log. This issue affects all versions of Junos OS Evolved prior to 19.3R1.	5.5	More Details
CVE-2020-1986	Improper input validation vulnerability in Secdo allows an authenticated local user with 'create folders or append data' access to the root of the OS disk (C:\) to cause a system crash on every login. This issue affects all versions Secdo for Windows.	5.5	More Details
CVE-2020-11723	Cellebrite UFED 5.0 through 7.29 uses four hardcoded RSA private keys to authenticate to the ADB daemon on target devices. Extracted keys can be used to place evidence onto target devices when performing a forensic extraction.	5.5	More Details
CVE-2020-11740	An issue was discovered in xenoprof in Xen through 4.13.x, allowing guest OS users (without active profiling) to obtain sensitive information about other guests. Unprivileged guests can request to map xenoprof buffers, even if profiling has not been enabled for those guests. These buffers were not scrubbed.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11742	An issue was discovered in Xen through 4.13.x, allowing guest OS users to cause a denial of service because of bad continuation handling in GNTTABOP_copy. Grant table operations are expected to return 0 for success, and a negative number for errors. The fix for CVE-2017-12135 introduced a path through grant copy handling where success may be returned to the caller without any action taken. In particular, the status fields of individual operations are left uninitialised, and may result in errant behaviour in the caller of GNTTABOP_copy. A buggy or malicious guest can construct its grant table in such a way that, when a backend domain tries to copy a grant, it hits the incorrect exit path. This returns success to the caller without doing anything, which may cause crashes or other incorrect behaviour.	5.5	More Details
CVE-2020-11743	An issue was discovered in Xen through 4.13.x, allowing guest OS users to cause a denial of service because of a bad error path in GNTTABOP_map_grant. Grant table operations are expected to return 0 for success, and a negative number for errors. Some misplaced brackets cause one error path to return 1 instead of a negative value. The grant table code in Linux treats this condition as success, and proceeds with incorrectly initialised state. A buggy or malicious guest can construct its grant table in such a way that, when a backend domain tries to map a grant, it hits the incorrect error path. This will crash a Linux based dom0 or backend domain.	5.5	More Details
CVE-2020-10977	GitLab EE/CE 8.5 to 12.9 is vulnerable to a an path traversal when moving an issue between projects.	5.5	More Details
CVE-2018-21076	An issue was discovered on Samsung mobile devices with N(7.x) (Exynos8890/8895 chipsets) software. There is information disclosure (a KASLR offset) in the Secure Driver via a modified trustlet. The Samsung ID is SVE-2017-10987 (April 2018).	5.5	More Details
CVE-2020-10814	A buffer overflow vulnerability in Code::Blocks 17.12 allows an attacker to execute arbitrary code via a crafted project file.	5.5	More Details
CVE-2020-5263	auth0.js (NPM package auth0-js) greater than version 8.0.0 and before version 9.12.3 has a vulnerability. In the case of an (authentication) error, the error object returned by the library contains the original request of the user, which may include the plaintext password the user entered. If the error object is exposed or logged without modification, the application risks password exposure. This is fixed in version 9.12.3	5.5	More Details
CVE-2020-11601	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. There is unauthorized access to applications in the Secure Folder via floating icons. The Samsung ID is SVE-2019-16195 (April 2020).	5.5	More Details
CVE-2020-11763	An issue was discovered in OpenEXR before 2.4.1. There is an std::vector out-of-bounds read and write, as demonstrated by ImfTileOffsets.cpp.	5.5	More Details
CVE-2020-11761	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds read during Huffman uncompression, as demonstrated by FastHufDecoder::refill in ImfFastHuf.cpp.	5.5	More Details
CVE-2020-11760	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds read during RLE uncompression in rleUncompress in ImfRle.cpp.	5.5	More Details
CVE-2020-8832	The fix for the Linux kernel in Ubuntu 18.04 LTS for CVE-2019-14615 ("The Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors.") was discovered to be incomplete, meaning that in versions of the kernel before 4.15.0-91.92, an attacker could use this vulnerability to expose sensitive information.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1801	There is an improper authentication vulnerability in several smartphones. Certain function interface in the system does not sufficiently validate the caller's identity in certain share scenario, successful exploit could cause information disclosure. Affected product versions include:Mate 30 Pro versions Versions earlier than 10.0.0.205(C00E202R7P2);Mate 30 versions Versions earlier than 10.0.0.205(C00E201R7P2).	5.5	More Details
CVE-2020-11759	An issue was discovered in OpenEXR before 2.4.1. Because of integer overflows in CompositeDeepScanLine::Data::handleDeepFrameBuffer and readSampleCountForLineBlock, an attacker can write to an out-of-bounds pointer.	5.5	More Details
CVE-2020-11758	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds read in ImfOptimizedPixelReading.h.	5.5	More Details
CVE-2020-11669	An issue was discovered in the Linux kernel before 5.2 on the powerpc platform. arch/powerpc/kernel/idle_book3s.S does not have save/restore functionality for PNV_POWERSAVE_AMR, PNV_POWERSAVE_UAMOR, and PNV_POWERSAVE_AMOR, aka CID-53a712bae5dd.	5.5	More Details
CVE-2020-11762	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds read and write in DwaCompressor::uncompress in ImfDwaCompressor.cpp when handling the UNKNOWN compression case.	5.5	More Details
CVE-2020-11764	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds write in copyIntoFrameBuffer in ImfMisc.cpp.	5.5	More Details
CVE-2020-9460	Octech Oempro 4.7 through 4.11 allow XSS by an authenticated user. The parameter CampaignName in Campaign.Create is vulnerable.	5.4	More Details
CVE-2020-6221	Web Intelligence HTML interface in SAP Business Objects Business Intelligence Platform, versions 4.1, 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	5.4	More Details
CVE-2020-6222	SAP Business Objects Business Intelligence Platform (Web Intelligence HTML interface), versions 4.1, 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	5.4	More Details
CVE-2020-4252	IBM DOORS Next Generation (DNG/RRC) 6.0.2. 6.0.6, and 6.0.61 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: 175490.	5.4	More Details
CVE-2020-6226	SAP Business Objects Business Intelligence Platform (Web Intelligence HTML interface), version 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	5.4	More Details
CVE-2020-6231	SAP Business Objects Business Intelligence Platform (Web Intelligence HTML interface), version 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	5.4	More Details
CVE-2019-4602	IBM Quality Manager (RQM) 6.02, 6.06, and 6.0.6.1 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: 168293.	5.4	More Details
CVE-2019-4737	IBM DOORS Next Generation (DNG/RRC) 6.0.2. 6.0.6, and 6.0.61 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: 172707.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-4740	IBM DOORS Next Generation (DNG/RRC) 6.0.2. 6.0.6, and 6.0.61 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: 172808.	5.4	More Details
CVE-2019-4746	IBM DOORS Next Generation (DNG/RRC) 6.0.2. 6.0.6, and 6.0.61 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: 172885.	5.4	More Details
CVE-2020-11714	eten PSG-6528VM 1.1 devices allow XSS via System Contact or System Location.	5.4	More Details
CVE-2020-4290	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could allow any authenticated user to spoof the configuration owner of any other user which disclose sensitive information or allow for unauthorized access. IBM X-Force ID: 176333.	5.4	More Details
CVE-2020-11556	An issue was discovered in Castle Rock SNMPc Online 12.10.10 before 2020-01-28. There are multiple persistent (stored) and reflected XSS vulnerabilities.	5.4	More Details
CVE-2020-9461	Octech Oempro 4.7 through 4.11 allow stored XSS by an authenticated user. The FolderName parameter of the Media.CreateFolder command is vulnerable.	5.4	More Details
CVE-2020-7802	The Synergy Systems & Solutions (SSS) HUSKY RTU 6049-E70, with firmware Versions 5.0 and prior, has an Incorrect Default Permissions (CWE-276) vulnerability. The affected product is vulnerable to insufficient default permissions, which could allow an attacker to view network configurations through SNMP communication. This is a different issue than CVE-2019-16879, CVE-2019-20045, CVE-2019-20046, CVE-2020-7800, and CVE-2020-7801.	5.3	More Details
CVE-2020-4284	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could disclose sensitive information to an unauthorized user due to insufficient timeout functionality in the Web UI. IBM X-Force ID: 176207.	5.3	More Details
CVE-2018-21067	An issue was discovered on Samsung mobile devices with M(6.0) software. There is an information disclosure in a Trustlet because an address is logged. The Samsung ID is SVE-2018-11600 (July 2018).	5.3	More Details
CVE-2020-11628	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. It is intended to support restriction of available remote protocols (CMP, ACME, REST, etc.) through the system configuration. These restrictions can be bypassed by modifying the URI string from a client. (EJBCA's internal access control restrictions are still in place, and each respective protocol must be configured to allow for enrollment.)	5.3	More Details
CVE-2020-11607	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Notification exposure occurs in Lockdown mode because of the Edge Lighting application. The Samsung ID is SVE-2020-16680 (April 2020).	5.3	More Details
CVE-2020-6232	SAP Commerce, versions 1811, 1905, does not perform necessary authorization checks for an anonymous user, due to Missing Authorization Check. This affects confidentiality of secure media.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4289	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 176332.	5.3	More Details
CVE-2020-7801	The Synergy Systems & Solutions (SSS) HUSKY RTU 6049-E70, with firmware Versions 5.0 and prior, has an Exposure of Sensitive Information to an Unauthorized Actor (CWE-200) vulnerability. The affected product is vulnerable to information exposure over the SNMP protocol. This is a different issue than CVE-2019-16879, CVE-2019-20045, CVE-2019-20046, CVE-2020-7800, and CVE-2020-7802.	5.3	More Details
CVE-2020-8148	UniFi Cloud Key firmware < 1.1.6 contains a vulnerability that enables an attacker being able to change a device hostname by sending a malicious API request. This affects Cloud Key gen2 and Cloud Key gen2 Plus.	5.3	More Details
CVE-2020-1616	Due to insufficient server-side login attempt limit enforcement, a vulnerability in the SSH login service of Juniper Networks Juniper Advanced Threat Prevention (JATP) Series and Virtual JATP (vJATP) devices allows an unauthenticated, remote attacker to perform multiple login attempts in excess of the configured login attempt limit. Successful exploitation will allow the attacker to perform brute-force password attacks on the SSH service. This issue affects: Juniper Networks JATP and vJATP versions prior to 5.0.6.0.	5.3	More Details
CVE-2020-11576	Fixed in v1.5.1, Argo version v1.5.0 was vulnerable to a user-enumeration vulnerability which allowed attackers to determine the usernames of valid (non-SSO) accounts because /api/v1/session returned 401 for an existing username and 404 otherwise.	5.3	More Details
CVE-2020-10978	GitLab EE/CE 8.11 to 12.9 is leaking information on Issues opened in a public project and then moved to a private project through Web-UI and GraphQL API.	5.3	More Details
CVE-2020-10381	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is an unauthenticated SQL injection in DATA24, allowing attackers to discover database and table names.	5.3	More Details
CVE-2020-1628	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It was discovered that packets utilizing these IP addresses may egress an EX4300 switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information exposure vulnerability. This issue affects Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D53 on EX4300; 15.1 versions prior to 15.1R7-S6 on EX4300; 15.1X49 versions prior to 15.1X49-D200, 15.1X49-D210 on EX4300; 16.1 versions prior to 16.1R7-S7 on EX4300; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on EX4300; 17.2 versions prior to 17.2R3-S3 on EX4300; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on EX4300; 17.4 versions prior to 17.4R2-S9, 17.4R3 on EX4300; 18.1 versions prior to 18.1R3-S8 on EX4300; 18.2 versions prior to 18.2R3-S2 on EX4300; 18.3 versions prior to 18.3R2-S3, 18.3R3, 18.3R3-S1 on EX4300; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on EX4300; 19.1 versions prior to 19.1R1-S4, 19.1R2 on EX4300; 19.2 versions prior to 19.2R1-S4, 19.2R2 on EX4300; 19.3 versions prior to 19.3R1-S1, 19.3R2 on EX4300.	5.3	More Details
CVE-2020-1730	A flaw was found in libssh versions before 0.8.9 and before 0.9.4 in the way it handled AES-CTR (or DES ciphers if enabled) ciphers. The server or client could crash when the connection hasn't been fully initialized and the system tries to cleanup the ciphers when closing the connection. The biggest threat from this vulnerability is system availability.	5.3	More Details
CVE-2020-11005	The WindowsHello open source library (NuGet HaemmerElectronics.SeppPenner.WindowsHello), before version 1.0.4, has a vulnerability where encrypted data could potentially be decrypted without needing authentication. If the library is used to encrypt text and write the output to a txt file, another executable could be able to decrypt the text using the static method NCryptDecrypt from this same library without the need to use Windows Hello Authentication again. This has been patched in version 1.0.4.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1630	A privilege escalation vulnerability in Juniper Networks Junos OS devices configured with dual Routing Engines (RE), Virtual Chassis (VC) or high-availability cluster may allow a local authenticated low-privileged user with access to the shell to perform unauthorized configuration modification. This issue does not affect Junos OS device with single RE or stand-alone configuration. This issue affects Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S14; 12.3X48 versions prior to 12.3X48-D86, 12.3X48-D90; 14.1X53 versions prior to 14.1X53-D51; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D181, 15.1X49-D190; 15.1X53 versions prior to 15.1X53-D592; 16.1 versions prior to 16.1R4-S13, 16.1R7-S6; 16.2 versions prior to 16.2R2-S10; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S6, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R2-S5, 18.2R3-S1; 18.2 versions prior to 18.2X75-D12, 18.2X75-D33, 18.2X75-D420, 18.2X75-D60, 18.2X75-D411; 18.3 versions prior to 18.3R1-S5, 18.3R2-S1, 18.3R3; 18.4 versions prior to 18.4R1-S4, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S2, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2.	5.0	More Details
CVE-2020-6218	Admin tools and Query Builder in SAP Business Objects Business Intelligence Platform, versions 4.1, 4.2, allows an attacker to access information that should otherwise be restricted, leading to Information Disclosure.	5.0	More Details
CVE-2020-8324	A vulnerability was reported in LenovoAppScenarioPluginSystem for Lenovo System Interface Foundation prior to version 1.2.184.31 that could allow unsigned DLL files to be executed.	5.0	More Details
CVE-2020-9500	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down.	4.9	More Details
CVE-2015-9546	An issue was discovered on Samsung mobile devices with KK(4.4) and later software through 2015-06-16. In some cases, HTTP is used for an Inputmethod, rather than HTTPS. A man-in-the-middle attacker can modify the client-server data stream to insert directory traversal sequences into an extracted file path. The Samsung ID is SVE-2015-4363 (November 2015).	4.8	More Details
CVE-2020-11003	Oasis before version 2.15.0 has a potential DNS rebinding or CSRF vulnerability. If you're running a vulnerable application on your computer and an attacker can trick you into visiting a malicious website, they could use DNS rebinding and CSRF attacks to read/write to vulnerable applications. This has been patched in 2.15.0.	4.8	More Details
CVE-2020-6214	SAP S/4HANA (Financial Products Subledger), version 100, uses an incorrect authorization object in some reports. Although the affected reports are protected with other authorization objects, exploitation of the vulnerability would allow an authenticated attacker to view, change, or delete data, thereby preventing the proper segregation of duties in the system.	4.7	More Details
CVE-2017-18646	An issue was discovered on Samsung mobile devices with M(6.x) and N(7.x) software. An attacker can bypass the password requirement for tablet user switching by folding the magnetic cover. The Samsung ID is SVE-2017-10602 (December 2017).	4.6	More Details
CVE-2020-1802	There is an insufficient integrity validation vulnerability in several products. The device does not sufficiently validate the integrity of certain file in certain loading processes, successful exploit could allow the attacker to load a crafted file to the device through USB.Affected product versions include:OSCA-550 versions 1.0.1.23(SP2);OSCA-550A versions 1.0.1.23(SP2);OSCA-550AX versions 1.0.1.23(SP2);OSCA-550X versions 1.0.1.23(SP2).	4.6	More Details
CVE-2018-21080	An issue was discovered on Samsung mobile devices with N(7.x) software. A physically proximate attacker wielding a magnet can activate NFC to bypass the lockscreen. The Samsung ID is SVE-2017-10897 (March 2018).	4.6	More Details
CVE-2018-21062	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. When biometric authentication is disabled, an attacker can view Streams content (e.g., a Gallery slideshow) of a locked Secure Folder via a connection to an external device. The Samsung ID is SVE-2018-11766 (August 2018).	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21053	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. There is Clipboard access in the lockscreen state via a physical keyboard. The Samsung ID is SVE-2018-12684 (October 2018).	4.6	More Details
CVE-2018-21056	An issue was discovered on Samsung mobile devices with O(8.x) software. The Smartwatch displays Secure Folder Notification content. The Samsung ID is SVE-2018-12458 (September 2018).	4.6	More Details
CVE-2020-8316	A vulnerability was reported in Lenovo Vantage prior to version 10.2003.10.0 that could allow an authenticated user to read files on the system with elevated privileges.	4.4	More Details
CVE-2020-10979	GitLab EE/CE 11.10 to 12.9 is leaking information on restricted CI pipelines metrics to unauthorized users.	4.3	More Details
CVE-2020-4282	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could allow an authenticated user to perform unauthorized actions by bypassing illegal character restrictions. X-Force ID: 176205.	4.3	More Details
CVE-2020-6435	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.	4.3	More Details
CVE-2019-4603	IBM Quality Manager (RQM) 6.02, 6.06, and 6.0.6.1 could allow an authenticated user to create keywords through the REST API and have them appear as if they were created by another user. IBM X-Force ID: 168295.	4.3	More Details
CVE-2020-6437	Inappropriate implementation in WebView in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to spoof security UI via a crafted application.	4.3	More Details
CVE-2020-6438	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension.	4.3	More Details
CVE-2020-6433	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	4.3	More Details
CVE-2020-6440	Inappropriate implementation in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information via a crafted Chrome Extension.	4.3	More Details
CVE-2020-6442	Inappropriate implementation in cache in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2020-6441	Insufficient policy enforcement in omnibox in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass security UI via a crafted HTML page.	4.3	More Details
CVE-2020-10981	GitLab EE/CE 9.0 to 12.9 allows a maintainer to modify other maintainers' pipeline trigger descriptions within the same project.	4.3	More Details
CVE-2020-4291	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could disclose sensitive information to an unauthorized user due to insufficient timeout functionality in the Web UI. IBM X-Force ID: 176334.	4.3	More Details
CVE-2020-6432	Insufficient policy enforcement in navigations in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	4.3	More Details
CVE-2020-6431	Insufficient policy enforcement in full screen in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to spoof security UI via a crafted HTML page.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6233	SAP S/4 HANA (Financial Products Subledger and Banking Services), versions - FSAPPL 400, 450, 500 and S4FPSL 100, allows an authenticated user to run an analysis report due to Missing Authorization Check, resulting in slowing the system.	4.3	More Details
CVE-2020-10975	GitLab EE/CE 10.8 to 12.9 is leaking metadata and comments on vulnerabilities to unauthorized users on the vulnerability feedback page.	4.3	More Details
CVE-2019-4601	IBM Quality Manager (RQM) 6.02, 6.06, and 6.0.6.1 could allow an authenticated user to obtain sensitive information from a stack trace that could aid in further attacks against the system.	4.3	More Details
CVE-2020-1988	An unquoted search path vulnerability in the Windows release of Global Protect Agent allows an authenticated local user with file creation privileges on the root of the OS disk (C:\) or to Program Files directory to gain system privileges. This issue affects Palo Alto Networks GlobalProtect Agent 5.0 versions before 5.0.5; 4.1 versions before 4.1.13 on Windows;	4.2	More Details
CVE-2020-9056	Periscope BuySpeed version 14.5 is vulnerable to stored cross-site scripting, which could allow a local, authenticated attacker to store arbitrary JavaScript within the application. This JavaScript is subsequently displayed by the application without sanitization and is executed in the browser of the user, which could possibly cause website redirection, session hijacking, or information disclosure. This vulnerability has been patched in BuySpeed version 15.3.	3.9	More Details
CVE-2020-11736	fr-archive-libarchive.c in GNOME file-roller through 3.36.1 allows Directory Traversal during extraction because it lacks a check of whether a file's parent is a symlink to a directory outside of the intended extraction location.	3.9	More Details
CVE-2020-1987	An information exposure vulnerability in the logging component of Palo Alto Networks Global Protect Agent allows a local authenticated user to read VPN cookie information when the troubleshooting logging level is set to "Dump". This issue affects Palo Alto Networks Global Protect Agent 5.0 versions prior to 5.0.9; 5.1 versions prior to 5.1.1.	3.9	More Details
CVE-2018-21074	An issue was discovered on Samsung mobile devices with M(6.x) (Exynos or Qualcomm chipsets) software. There is information disclosure from a Trustlet via the debug log. The Samsung ID is SVE-2017-10638 (April 2018).	3.3	More Details
CVE-2018-21043	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos 9810 chipsets) software. There is information disclosure about a kernel pointer in the g2d_drv driver because of logging. The Samsung ID is SVE-2018-13035 (December 2018).	3.3	More Details
CVE-2020-5303	Tendermint before versions 0.33.3, 0.32.10, and 0.31.12 has a denial-of-service vulnerability. Tendermint does not limit the number of P2P connection requests. For each p2p connection, it allocates XXX bytes. Even though this memory is garbage collected once the connection is terminated (due to duplicate IP or reaching a maximum number of inbound peers), temporary memory spikes can lead to OOM (Out-Of-Memory) exceptions. Additionally, Tendermint does not reclaim activeID of a peer after it's removed in Mempool reactor. This does not happen all the time. It only happens when a connection fails (for any reason) before the Peer is created and added to all reactors. RemovePeer is therefore called before AddPeer, which leads to always growing memory (activeIDs map). The activeIDs map has a maximum size of 65535 and the node will panic if this map reaches the maximum. An attacker can create a lot of connection attempts (exploiting above denial of service), which ultimately will lead to the node panicking. These issues are patched in Tendermint 0.33.3 and 0.32.10.	3.1	More Details
CVE-2019-1866	Cisco Webex Business Suite before 39.1.0 contains a vulnerability that could allow an unauthenticated, remote attacker to affect the integrity of the application. The vulnerability is due to improper validation of host header values. An attacker with a privileged network position, either a man-in-the-middle or by intercepting wireless network traffic, could exploit this vulnerability to manipulate header values sent by a client to the affected application. The attacker could cause the application to use input from the header to redirect a user from the Cisco Webex Meetings Online site to an arbitrary site of the attacker's choosing.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3126	vulnerability within the Multimedia Viewer feature of Cisco Webex Meetings could allow an authenticated, remote attacker to bypass security protections. The vulnerability is due to missing security warning dialog boxes when a room host views shared multimedia files. An authenticated, remote attacker could exploit this vulnerability by using the host role to share files within the Multimedia sharing feature and convincing a former room host to view that file. A warning dialog normally appears cautioning users before the file is displayed; however, the former host would not see that warning dialog, and any shared multimedia would be rendered within the user's browser. The attacker could leverage this behavior to conduct additional attacks by including malicious files within a targeted room host's browser window.	3.0	More Details
CVE-2020-4164	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could expose sensitive information from applicatino errors which could be used in further attacks against the system. IBM X-Force ID: 174400.	2.7	More Details
CVE-2018-21073	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.0) (Galaxy S9+, Galaxy S9, Galaxy S8+, Galaxy S8, Note 8). There is access to Clipboard content in the locked state via the Edge panel. The Samsung ID is SVE-2017-10748 (May 2018).	2.4	More Details
CVE-2018-21046	An issue was discovered on Samsung mobile devices with O(8.x) software. There is clipboard Data Exposure via the Emergency Dialer upon connecting a USB device. The Samsung ID is SVE-2018-12911 (November 2018).	2.4	More Details
CVE-2020-11602	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Google Assistant leaks clipboard contents on a locked device. The Samsung ID is SVE-2019-16558 (April 2020).	2.4	More Details
CVE-2020-11606	An issue was discovered on Samsung mobile devices with Q(10.0) software. Information about application preview (in the Secure Folder) leaks on a locked device. The Samsung ID is SVE-2019-16463 (April 2020).	2.4	More Details
CVE-2018-21077	An issue was discovered on Samsung mobile devices with M(6.0), N(7.x), and O(8.x) software. There is a Clipboard content disclosure in the locked state because the keyboard may be used during an emergency call. The Samsung ID is SVE-2017-11107 (April 2018).	2.4	More Details