SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 09 September 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-2020-1889	A security feature bypass issue in WhatsApp Desktop versions prior to v0.3.4932 could have allowed for sandbox escape in Electron and escalation of privilege if combined with a remote code execution vulnerability inside the sandboxed renderer process.	10.0	More Details
CVE-2020-3495	A vulnerability in Cisco Jabber for Windows could allow an authenticated, remote attacker to execute arbitrary code. The vulnerability is due to improper validation of message contents. An attacker could exploit this vulnerability by sending specially crafted Extensible Messaging and Presence Protocol (XMPP) messages to the affected software. A successful exploit could allow the attacker to cause the application to execute arbitrary programs on the targeted system with the privileges of the user account that is running the Cisco Jabber client software, possibly resulting in arbitrary code execution.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24355	Zyxel VMG5313-B30B router on firmware 5.13(ABCJ.6)b3_1127, and possibly older versions of firmware are affected by insecure permissions which allows regular and other users to create new users with elevated privileges. This is done by changing "FirstIndex" field in JSON that is POST-ed during account creation. Similar may also be possible with account deletion.	9.8	More Details
CVE-2020-3669	u'Buffer Overflow issue in WLAN tcp ip verification due to usage of out of range pointer offset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130	9.8	More Details
CVE-2020-3668	u'Buffer overflow while parsing PMF enabled MCBC frames due to frame length being lesser than what is expected while parsing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2020-3667	u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130	9.8	More Details
CVE-2020-11117	u'In the lbd service, an external user can issue a specially crafted debug command to overwrite arbitrary files with arbitrary content resulting in remote code execution.' in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA4531, QCA9531, QCA9980	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11116	u'Possible out of bound write while processing association response received from host due to lack of check of IE length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	9.8	More Details
CVE-2019-14052	u'Accessing an uninitialized data structure could result in partially copying of contents and thus incorrect processing' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, SA415M, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2020-24987	Tenda AC18 Router through V15.03.05.05_EN and through V15.03.05.19(6318) CN devices could cause a remote code execution due to incorrect authentication handling of vulnerable logincheck() function in /usr/lib/lua/ngx_authserver/ngx_wdas.lua file if the administrator UI Interface is set to "radius".	9.8	More Details
CVE-2020-7730	The package bestzip before 2.1.7 are vulnerable to Command Injection via the options param.	9.8	More Details
CVE-2020-25023	An issue was discovered in Noise-Java through 2020-08-27. AESGCMOnCtrCipherState.encryptWithAd() allows out-of-bounds access.	9.8	More Details
CVE-2020-25022	An issue was discovered in Noise-Java through 2020-08-27. AESGCMFallbackCipherState.encryptWithAd() allows out-of-bounds access.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25021	An issue was discovered in Noise-Java through 2020-08-27. ChaChaPolyCipherState.encryptWithAd() allows out-of-bounds access.	9.8	More Details
CVE-2020-1911	A type confusion vulnerability when resolving properties of JavaScript objects with specially-crafted prototype chains in Facebook Hermes prior to commit fe52854cdf6725c2eaa9e125995da76e6ceb27da allows attackers to potentially execute arbitrary code via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected.	9.8	More Details
CVE-2020-13802	Rebar3 versions 3.0.0-beta.3 to 3.13.2 are vulnerable to OS command injection via URL parameter of dependency specification.	9.8	More Details
CVE-2020-24978	In NASM 2.15.04rc3, there is a double-free vulnerability in pp_tokline asm/preproc.c. This is fixed in commit 8806c3ca007b84accac21dd88b900fb03614ceb7.	9.8	More Details
CVE-2020-25006	Heybbs v1.2 has a SQL injection vulnerability in login.php file via the username parameter which may allow a remote attacker to execute arbitrary code.	9.8	More Details
CVE-2020-25005	Heybbs v1.2 has a SQL injection vulnerability in msg.php file via the ID parameter which may allow a remote attacker to execute arbitrary code.	9.8	More Details
CVE-2020-25004	Heybbs v1.2 has a SQL injection vulnerability in user.php file via the ID parameter which may allow a remote attacker to execute arbitrary code.	9.8	More Details
CVE-2020-1891	A user controlled parameter used in video call in WhatsApp for Android prior to v2.20.17, WhatsApp Business for Android prior to v2.20.7, WhatsApp for iPhone prior to v2.20.20, and WhatsApp Business for iPhone prior to v2.20.20 could have allowed an out-of-bounds write on 32-bit devices.	9.8	More Details
CVE-2020-24193	A SQL injection vulnerability in login in Sourcecodetester Daily Tracker System 1.0 allows unauthenticated user to execute authentication bypass with SQL injection via the email parameter.	9.8	More Details
CVE-2020-24876	Use of a hard-coded cryptographic key in Pancake versions < 4.13.29 allows an attacker to forge session cookies, which may lead to remote privilege escalation.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25105	eramba c2.8.1 and Enterprise before e2.19.3 has a weak password recovery token (createHash has only a million possibilities).	9.8	More Details
CVE-2020-4693	IBM Spectrum Protect Operations Center 7.1.0.000 through 7.1.10 and 8.1.0.000 through 8.1.9 may allow an attacker to execute arbitrary code on the system, caused by improper validation of data prior to export. IBM X-Force ID: 186782.	9.8	More Details
CVE-2020-24030	ForLogic Qualiex v1 and v3 has weak token expiration. This allows remote unauthenticated privilege escalation and access to sensitive data via token reuse.	9.8	More Details
CVE-2020-24029	Because of unauthenticated password changes in ForLogic Qualiex v1 and v3, customer and admin permissions and data can be accessed via a simple request.	9.8	More Details
CVE-2020-3675	u'Potential integer underflow while parsing Service Info and IPv6 link-local TLVs that comes as part of NDPE attribute' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ5018, IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCN7605, QCS404, QCS405, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250	9.8	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-5369	Dell EMC Isilon OneFS versions 8.2.2 and earlier and Dell EMC PowerScale OneFS version 9.0.0 contain a privilege escalation vulnerability. An authenticated malicious user may exploit this vulnerability by using SyncIQ to gain unauthorized access to system management files.	8.8	More Details
CVE-2020-14209	Dolibarr before 11.0.5 allows low-privilege users to upload files of dangerous types, leading to arbitrary code execution. This occurs because .pht and .phar files can be uploaded. Also, a .htaccess file can be uploaded to reconfigure access control (e.g., to let .noexe files be executed as PHP code to defeat the .noexe protection mechanism).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12248	In Foxit Reader and PhantomPDF before 10.0.1, and PhantomPDF before 9.7.3, attackers can execute arbitrary code via a heap-based buffer overflow because dirty image-resource data is mishandled.	8.8	More Details
CVE-2020-3430	A vulnerability in the application protocol handling features of Cisco Jabber for Windows could allow an unauthenticated, remote attacker to execute arbitrary commands. The vulnerability is due to improper handling of input to the application protocol handlers. An attacker could exploit this vulnerability by convincing a user to click a link within a message sent by email or other messaging platform. A successful exploit could allow the attacker to execute arbitrary commands on a targeted system with the privileges of the user account that is running the Cisco Jabber client software.	8.8	More Details
CVE-2020-24949	Privilege escalation in PHP-Fusion 9.03.50 downloads/downloads.php allows an authenticated user (not admin) to send a crafted request to the server and perform remote command execution (RCE).	8.8	More Details
CVE-2020-23834	Insecure Service File Permissions in the bd service in Real Time Logic BarracudaDrive v6.5 allow local attackers to escalate privileges to admin by replacing the %SYSTEMDRIVE%\bd\bd.exe file. When the computer next starts, the new bd.exe will be run as LocalSystem.	8.8	More Details
CVE-2020-1894	A stack write overflow in WhatsApp for Android prior to v2.20.35, WhatsApp Business for Android prior to v2.20.20, WhatsApp for iPhone prior to v2.20.30, and WhatsApp Business for iPhone prior to v2.20.30 could have allowed arbitrary code execution when playing a specially crafted push to talk message.	8.8	More Details
CVE-2020-24028	ForLogic Qualiex v1 and v3 allows any authenticated customer to achieve privilege escalation via user creations, password changes, or user permission updates.	8.8	More Details
CVE-2020-1886	A buffer overflow in WhatsApp for Android prior to v2.20.11 and WhatsApp Business for Android prior to v2.20.2 could have allowed an out-of-bounds write via a specially crafted video stream after receiving and answering a malicious video call.	8.8	More Details
CVE-2020-25079	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. cgi-bin/ddns_enc.cgi allows authenticated command injection.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3530	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to execute that command, even though administrative privileges should be required. The attacker must have valid credentials on the affected device. The vulnerability is due to incorrect mapping in the source code of task group assignments for a specific command. An attacker could exploit this vulnerability by issuing the command, which they should not be authorized to issue, on an affected device. A successful exploit could allow the attacker to invalidate the integrity of the disk and cause the device to restart. This vulnerability could allow a user with read permissions to issue a specific command that should require Administrator privileges.	8.4	More Details
CVE-2020-15167	In Miller (command line utility) using the configuration file support introduced in version 5.9.0, it is possible for an attacker to cause Miller to run arbitrary code by placing a malicious `.mlrrc` file in the working directory. See linked GitHub Security Advisory for complete details. A fix is ready and will be released as Miller 5.9.1.	8.2	More Details
CVE-2018-13903	u'Error in UE due to race condition in EPCO handling' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, MDM9205, MDM9206, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, SDM450, SM8150	8.1	More Details
CVE-2020-3478	A vulnerability in the REST API of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker to overwrite certain files that should be restricted on an affected device. The vulnerability is due to insufficient authorization enforcement on an affected system. An attacker could exploit this vulnerability by uploading a file using the REST API. A successful exploit could allow an attacker to overwrite and upload files, which could degrade the functionality of the affected system.	8.1	More Details
CVE-2020-11493	In Foxit Reader and PhantomPDF before 10.0.1, and PhantomPDF before 9.7.3, attackers can obtain sensitive information about an uninitialized object because of direct transformation from PDF Object to Stream without concern for a crafted XObject.	8.1	More Details
CVE-2020-16602	Razer Chroma SDK Rest Server through 3.12.17 allows remote attackers to execute arbitrary programs because there is a race condition in which a file created under "%PROGRAMDATA%\Razer Chroma\SDK\Apps" can be replaced before it is executed by the server. The attacker must have access to port 54236 for a registration step.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15094	In Symfony before versions 4.4.13 and 5.1.5, the CachingHttpClient class from the HttpClient Symfony component relies on the HttpCache class to handle requests. HttpCache uses internal headers like X-Body-Eval and X-Body-File to control the restoration of cached responses. The class was initially written with surrogate caching and ESI support in mind (all HTTP calls come from a trusted backend in that scenario). But when used by CachingHttpClient and if an attacker can control the response for a request being made by the CachingHttpClient, remote code execution is possible. This has been fixed in versions 4.4.13 and 5.1.5.	8.0	More Details
CVE-2020-11120	u'Calling thread may free the data buffer pointer that was passed to the callback and later when event loop executes the callback, data buffer may not be valid and will lead to use after free scenario' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, APQ8098, Bitra, Kamorta, MSM8917, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM632, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2020-25125	GnuPG 2.2.21 and 2.2.22 (and Gpg4win 3.1.12) has an array overflow, leading to a crash or possibly unspecified other impact, when a victim imports an attacker's OpenPGP key, and this key has AEAD preferences. The overflow is caused by a g10/key-check.c error. NOTE: GnuPG 2.3.x is unaffected. GnuPG 2.2.23 is a fixed version.	7.8	More Details
CVE-2020-11128	u'Possible out of bound access while copying the mask file content into the buffer without checking the buffer size' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9607, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCM2150, QCS405, QCS605, QCS610, QM215, Rennell, SA515M, SA6155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-24996	There is an invalid memory access in the function TextString::~TextString() located in Catalog.cc in Xpdf 4.0.2. It can be triggered by (for example) sending a crafted pdf file to the pdftohtml binary, which allows a remote attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24161	Guangzhou NetEase Mail Master 4.14.1.1004 on Windows has a DLL hijacking vulnerability. Attackers can use this vulnerability to execute malicious code.	7.8	More Details
CVE-2020-11133	u'Possible out of bound array write in rxdco cal utility due to lack of array bound check' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MSM8998, QCS605, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130	7.8	More Details
CVE-2020-24999	There is an invalid memory access in the function fprintf located in Error.cc in Xpdf 4.0.2. It can be triggered by sending a crafted PDF file to the pdftohtml binary, which allows a remote attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact.	7.8	More Details
CVE-2020-3622	u'Channel name string which has been read from shared memory is potentially subjected to string manipulations but not validated for NULL termination can results into memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3624	u'A potential buffer overflow exists due to integer overflow when parsing handler options due to wrong data type usage in operation' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	7.8	More Details
CVE-2020-24162	The Shenzhen Tencent app 5.8.2.5300 for PC platforms (from Tencent App Center) has a DLL hijacking vulnerability. Attackers can use this vulnerability to execute malicious code.	7.8	More Details
CVE-2019-13992	u'Out of bound memory access if stack push and pop operation are performed without doing a bound check on stack top' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, IPQ6018, IPQ8074, MDM9205, Nicobar, QCA8081, QCN7605, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-24160	Shenzhen Tencent TIM Windows client 3.0.0.21315 has a DLL hijacking vulnerability, which can be exploited by attackers to execute malicious code.	7.8	More Details
CVE-2020-24159	NetEase Youdao Dictionary has a DLL hijacking vulnerability, which can be exploited by attackers to gain server permissions. This affects Guangzhou NetEase Youdao Dictionary 8.9.2.0.	7.8	More Details
CVE-2020-24158	360 Speed Browser 12.0.1247.0 has a DLL hijacking vulnerability, which can be exploited by attackers to execute malicious code. It is a dual-core browser owned by Beijing Qihoo Technology.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3629	u'Stack out of bound issue occurs when making query to DSP capabilities due to wrong assumption was made on determining the buffer size for the DSP attributes' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, Kamorta, Rennell, SC7180, SDM845, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2020-3611	u'XBL SEC clears only ZI region when loading Qualcomm-signed segments can lead to improper access issue' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SXR1130	7.8	More Details
CVE-2019-14089	u'Keymaster attestation key and device IDs provisioning which is a one time process is incorrectly allowed to be re-provisioned after a user data erase or a factory reset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, Nicobar, QCS404, QCS610, Rennell, SA515M, SA6155P, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2019-14117	u'Whenever the page list is updated via privileged user, the previous list elements are freed but are not deleted from the list which results in a use after free causing an unhandled page fault exception in rmnet driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MDM9607, QCS405, Saipan, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2020-3473	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local CLI shell user to elevate privileges and gain full administrative control of the device. The vulnerability is due to incorrect mapping of a command to task groups within the source code. An attacker could exploit this vulnerability by first authenticating to the local CLI shell on the device and using the CLI command to bypass the task group–based checks. A successful exploit could allow the attacker to elevate privileges and perform actions on the device without authorization checks.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10628	u'Memory can be potentially corrupted if random index is allowed to manipulate TLB entries in Kernel from user library' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8098, Bitra, MDM9205, MDM9650, MSM8998, Nicobar, QCA6390, QCN7605, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-10615	u'Possibility of integer overflow in keymaster 4 while allocating memory due to multiplication of large numcerts value and size of keymaster bob which can lead to memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-10596	u'Improper access control can lead signed process to guess pid of other processes and access their address space' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Nicobar, QCS605, QCS610, Rennell, SA6155P, Saipan, SC7180, SC8180X, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10562	u'Improper authentication and signature verification of debug polices in secure boot loader will allow unverified debug policies to be loaded into secure memory and leads to memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, Kamorta, MSM8998, Nicobar, QCS404, QCS605, QCS610, Rennell, SA415M, SA6155P, SC7180, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-10527	u'SMEM partition can be manipulated in case of any compromise on HLOS, thus resulting in access to memory outside of SMEM address range which could lead to memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA4531, QCA6574AU, QCA8081, QCM2150, QCN7605, QCN7606, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-13994	u'Lack of check that the current received data fragment size of a particular packet that are read from shared memory are less than the actual packet size can lead to memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-13995	u'Lack of integer overflow check for addition of fragment size and remaining size that are read from shared memory can lead to memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-13998	u'Lack of check that the TX FIFO write and read indices that are read from shared RAM are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-13999	u'Lack of check for integer overflow for round up and addition operations result into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-4545	IBM Aspera Connect 3.9.9 could allow a remote attacker to execute arbitrary code on the system, caused by improper loading of Dynamic Link Libraries by the import feature. By persuading a victim to open a specially-crafted .DLL file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183190.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-3881	Bundler prior to 2.1.0 uses a predictable path in /tmp/, created with insecure permissions as a storage location for gems, if locations under the user's home directory are not available. If Bundler is used in a scenario where the user does not have a writable home directory, an attacker could place malicious code in this directory that would be later loaded and executed.	7.8	More Details
CVE-2019-14056	u'Possible integer overflow in API due to lack of check on large oid range count in cert extension field' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9150, MDM9205, MDM9607, MDM9650, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	7.8	More Details
CVE-2019-14065	u'Pointer double free in HavenSvc due to not setting the pointer to NULL after freeing it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-14074	u'Heap overflow in diag command handler due to lack of check of packet length received from user' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10679	Thomson Reuters Eikon 4.0.42144 allows all local users to modify the service executable file because of weak %PROGRAMFILES(X86)%\Thomson Reuters\Eikon permissions.	7.8	More Details
CVE-2020-3636	u'Out of bound writes happen when accessing usage_table header entry beyond the memory allocated for the header' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130	7.8	More Details
CVE-2019-10629	u'User Process can potentially corrupt kernel virtual page by passing a crafted page in API' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, IPQ6018, IPQ8074, MDM9205, Nicobar, QCA8081, QCN7605, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-3646	u'Buffer overflow seen as the destination buffer size is lesser than the source buffer size in video application' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Bitra, MSM8909W, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDA845, SDM429W, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2020-7830	RAONWIZ v2018.0.2.50 and earlier versions contains a vulnerability that could allow remote files to be downloaded by lack of validation. Vulnerabilities in downloading with Kupload agent allow files to be downloaded to arbitrary paths due to insufficient verification of extensions and download paths. This issue affects: RAONWIZ RAON KUpload 2018.0.2.50 versions and earlier.	7.8	More Details
CVE-2020-3648	u'Possible out of bound write in DSP driver code due to lack of check of data received from user' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3666	u'Out of bounds memory access during memory copy while processing Host command' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5500, QCN5502, QCS404, QCS405, QCS605, SA6155P, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SXR1130	7.8	More Details
CVE-2020-3640	u'Resizing the usage table header before passing all the checks leads to the function exiting with a usage table in invalid state when a HLOS adversary calls the function with wrong input' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, QCS404, QCS610, Rennell, Saipan, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130	7.8	More Details
CVE-2020-25045	Installers of Kaspersky Security Center and Kaspersky Security Center Web Console prior to 12 & prior to 12 Patch A were vulnerable to a DLL hijacking attack that allowed an attacker to elevate privileges in the system.	7.8	More Details
CVE-2020-3647	u'Potential buffer overflow when accessing npu debugfs node "off"/"log" with large buffer size' in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, SC8180X, SDX55, SM6150, SM7150, SM8150	7.8	More Details
CVE-2020-5420	Cloud Foundry Routing (Gorouter) versions prior to 0.206.0 allow a malicious developer with "cf push" access to cause denial-of-service to the CF cluster by pushing an app that returns specially crafted HTTP responses that crash the Gorouters.	7.7	More Details
CVE-2020-5778	A flaw exists in Trading Technologies Messaging 7.1.28.3 (ttmd.exe) due to improper validation of user-supplied data when processing a type 8 message sent to default TCP RequestPort 10200. An unauthenticated, remote attacker can exploit this issue, via a specially crafted message, to terminate ttmd.exe.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5779	A flaw in Trading Technologies Messaging 7.1.28.3 (ttmd.exe) relates to invalid parameter handling when calling strcpy_s() with an invalid parameter (i.e., a long src string parameter) as a part of processing a type 4 message sent to default TCP RequestPort 10200. It's been observed that ttmd.exe terminates as a result.	7.5	More Details
CVE-2020-11118	u'Information exposure issues while processing IE header due to improper check of beacon IE frame' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QCS610, QM215, Rennell, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.5	More Details
CVE-2020-11158	u'Null pointer dereference in HP OfficeJet Pro 8210 jbig2 filter due to lack of check of PDF font array leads to denial of service' in IPS PDF releases prior to IPS System 2020.2	7.5	More Details
CVE-2020-24940	An issue was discovered in Laravel before 6.18.34 and 7.x before 7.23.2. Unvalidated values are saved to the database in some situations in which table names are stripped during a mass assignment.	7.5	More Details
CVE-2020-11115	u'Buffer over read occurs while processing information element from beacon due to lack of check of data received from beacon' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5622	Shadankun Server Security Type (excluding normal blocking method types) Ver.1.5.3 and earlier allows remote attackers to cause a denial of service which may result in not being able to add newly detected attack source IP addresses as blocking targets for about 10 minutes via a specially crafted request.	7.5	More Details
CVE-2020-5386	Dell EMC ECS, versions prior to 3.5, contains an Exposure of Resource vulnerability. A remote unauthenticated attacker can access the list of DT (Directory Table) objects of all internally running services and gain knowledge of sensitive data of the system.	7.5	More Details
CVE-2020-24941	An issue was discovered in Laravel before 6.18.35 and 7.x before 7.24.0. The $guarded property is mishandled in some situations involving requests with JSON column nesting expressions.	7.5	More Details
CVE-2020-11579	An issue was discovered in Chadha PHPKB 9.0 Enterprise Edition. installer/test-connection.php (part of the installation process) allows a remote unauthenticated attacker to disclose local files on hosts running PHP before 7.2.16, or on hosts where the MySQL ALLOW LOCAL DATA INFILE option is enabled.	7.5	More Details
CVE-2020-1890	A URL validation issue in WhatsApp for Android prior to v2.20.11 and WhatsApp Business for Android prior to v2.20.2 could have caused the recipient of a sticker message containing deliberately malformed data to load an image from a sender-controlled URL without user interaction.	7.5	More Details
CVE-2020-25068	Setelsa Conacwin v3.7.1.2 is vulnerable to a local file inclusion vulnerability. This vulnerability allows a remote unauthenticated attacker to read internal files on the server via an http:IP:PORT/../../path/file_to_disclose Directory Traversal URI. NOTE: The manufacturer indicated that the affected version does not exist. Furthermore, they indicated that they detected this problem in an internal audit more than 3 years ago and fixed it in 2017.	7.5	More Details
CVE-2020-25078	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. The unauthenticated /config/getuser endpoint allows for remote administrator password disclosure.	7.5	More Details
CVE-2019-20916	The pip package before 19.2 for Python allows Directory Traversal when a URL is given in an install command, because a Content-Disposition header can have ../ in a filename, as demonstrated by overwriting the /root/.ssh/authorized_keys file. This occurs in _download_http_url in _internal/download.py.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23811	xxl-job 2.2.0 allows Information Disclosure of username, model, and password via job/admin/controller/UserController.java.	7.5	More Details
CVE-2020-24659	An issue was discovered in GnuTLS before 3.6.15. A server can trigger a NULL pointer dereference in a TLS 1.3 client if a no_renegotiation alert is sent with unexpected timing, and then an invalid second handshake occurs. The crash happens in the application's error handling path, where the gnutls_deinit function is called after detecting a handshake failure.	7.5	More Details
CVE-2020-4638	IBM API Connect's API Manager 2018.4.1.0 through 2018.4.1.12 is vulnerable to privilege escalation. An invitee to an API Provider organization can escalate privileges by manipulating the invitation link. IBM X-Force ID: 185508.	7.2	More Details
CVE-2020-24986	Concrete5 up to and including 8.5.2 allows Unrestricted Upload of File with Dangerous Type such as a .php file via File Manager. It is possible to modify site configuration to upload the PHP file and execute arbitrary commands.	7.2	More Details
CVE-2020-14008	Zoho ManageEngine Applications Manager 14710 and before allows an authenticated admin user to upload a vulnerable jar in a specific location, which leads to remote code execution.	7.2	More Details
CVE-2020-24948	The ao_ccss_import AJAX call in Autoptimize Wordpress Plugin 2.7.6 does not ensure that the file provided is a legitimate Zip file, allowing high privilege users to upload arbitrary files, such as PHP, leading to remote command execution.	7.2	More Details
CVE-2020-25042	An arbitrary file upload issue exists in Mara CMS 7.5. In order to exploit this, an attacker must have a valid authenticated (admin/manager) session and make a codebase/dir.php?type=filenew request to upload PHP code to codebase/handler.php.	7.2	More Details
CVE-2020-12247	In Foxit Reader and PhantomPDF before 10.0.1, and PhantomPDF before 9.7.3, attackers can obtain sensitive information from an out-of-bounds read because a text-string index continues to be used after splitting a string into two parts. A crash may also occur.	7.1	More Details
CVE-2020-23830	A Cross-Site Request Forgery (CSRF) vulnerability in changeUsername.php in SourceCodester Stock Management System v1.0 allows remote attackers to deny future logins by changing an authenticated victim's username when they visit a third-party site.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7729	The package grunt before 1.3.0 are vulnerable to Arbitrary Code Execution due to the default usage of the function load() instead of its secure replacement safeLoad() of the package js-yaml inside grunt.file.readYAML.	7.1	More Details
CVE-2020-25044	Kaspersky Virus Removal Tool (KVRT) prior to 15.0.23.0 was vulnerable to arbitrary file corruption that could provide an attacker with the opportunity to eliminate content of any file in the system.	7.1	More Details
CVE-2020-25043	The installer of Kaspersky VPN Secure Connection prior to 5.0 was vulnerable to arbitrary file deletion that could allow an attacker to delete any file in the system.	7.1	More Details
CVE-2020-3619	u'Non-secure memory is touched multiple times during TrustZone\u2019s execution and can lead to privilege escalation or memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ8074, Kamorta, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, QCA8081, QCS404, QCS605, QCS610, QM215, Rennell, SA415M, SC7180, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130	7.0	More Details
CVE-2019-14119	u'While processing SMCInvoke asynchronous message header, message count is modified leading to a TOCTOU race condition and lead to memory corruption' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, Kamorta, MDM9205, MDM9607, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDM670, SDM710, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.0	More Details
CVE-2020-5378	Dell G7 17 7790 BIOS versions prior to 1.13.2 contain a UEFI BIOS Boot Services overwrite vulnerability. A local attacker with access to system memory may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in System Management Mode (SMM).	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5376	Dell Inspiron 7347 BIOS versions prior to A13 contain a UEFI BIOS Boot Services overwrite vulnerability. A local attacker with access to system memory may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in System Management Mode (SMM).	6.8	More Details
CVE-2020-7382	Rapid7 Nexpose installer version prior to 6.6.40 contains an Unquoted Search Path which may allow an attacker on the local machine to insert an arbitrary file into the executable path. This issue affects: Rapid7 Nexpose versions prior to 6.6.40.	6.8	More Details
CVE-2020-5379	Dell Inspiron 7352 BIOS versions prior to A12 contain a UEFI BIOS Boot Services overwrite vulnerability. A local attacker with access to system memory may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in System Management Mode (SMM).	6.8	More Details
CVE-2020-9199	B2368-22 V100R001C00;B2368-57 V100R001C00;B2368-66 V100R001C00 have a command injection vulnerability. An attacker with high privileges may exploit this vulnerability through some operations on the LAN. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject commands to the target device.	6.8	More Details
CVE-2020-15810	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Smuggling attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the proxy cache and any downstream caches with content from an arbitrary source. When configured for relaxed header parsing (the default), Squid relays headers containing whitespace characters to upstream servers. When this occurs as a prefix to a Content-Length header, the frame length specified will be ignored by Squid (allowing for a conflicting length to be used from another Content-Length header) but relayed upstream.	6.5	More Details
CVE-2020-3702	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4632	IBM InfoSphere Metadata Asset Manager 11.7 is vulnerable to server-side request forgery. By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to submit or control server requests. IBM X-Force ID: 185416.	6.5	More Details
CVE-2020-3498	A vulnerability in Cisco Jabber software could allow an authenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper validation of message contents. An attacker could exploit this vulnerability by sending specially crafted messages to a targeted system. A successful exploit could allow the attacker to cause the application to return sensitive authentication information to another system, possibly for use in further attacks.	6.5	More Details
CVE-2020-15811	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Splitting attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the browser cache and any downstream caches with content from an arbitrary source. Squid uses a string search instead of parsing the Transfer-Encoding header to find chunked encoding. This allows an attacker to hide a second request inside Transfer-Encoding: it is interpreted by Squid as chunked and split out into a second request delivered upstream. Squid will then deliver two distinct responses to the client, corrupting any downstream caches.	6.5	More Details
CVE-2020-4337	IBM API Connect 2018.4.1.0 through 2018.4.1.12 could allow an attacker to launch phishing attacks by tricking the server to generate user registration emails that contain malicious URLs. IBM X-Force ID: 177933.	6.5	More Details
CVE-2020-24977	GNOME project libxml2 v2.9.10 has a global buffer over-read vulnerability in xmlEncodeEntitiesInternal at libxml2/entities.c. The issue has been fixed in commit 50f06b3e.	6.5	More Details
CVE-2020-12621	The Teamwire application 5.3.0 for Android allows physically proximate attackers to exploit a flaw related to the pass-code component.	6.1	More Details
CVE-2020-13972	Enghouse Web Chat 6.2.284.34 allows XSS. When one enters their own domain name in the WebServiceLocation parameter, the response from the POST request is displayed, and any JavaScript returned from the external server is executed in the browser. This is related to CVE-2019-16951.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25102	silverstripe-advancedreports (aka the Advanced Reports module for SilverStripe) 1.0 through 2.0 is vulnerable to Cross-Site Scripting (XSS) because it is possible to inject and store malicious JavaScript code. The affects admin/advanced-reports/DataObjectReport/EditForm/field/DataObjectReport/item (aka report preview) when an SVG document is provided in the Description parameter.	6.1	More Details
CVE-2020-23814	Multiple cross-site scripting (XSS) vulnerabilities in xxl-job v2.2.0 allow remote attackers to inject arbitrary web script or HTML via (1) AppName and (2)AddressList parameter in JobGroupController.java file.	6.1	More Details
CVE-2020-24604	A Reflected XSS vulnerability was discovered in Ignite Realtime Openfire version 4.5.1. The XSS vulnerability allows remote attackers to inject arbitrary web script or HTML via the GET request "searchName", "searchValue", "searchDescription", "searchDefaultValue","searchPlugin", "searchDescription" and "searchDynamic" in server-properties.jsp and security-audit-viewer.jsp	6.1	More Details
CVE-2020-24602	Ignite Realtime Openfire 4.5.1 has a reflected Cross-site scripting vulnerability which allows an attacker to execute arbitrary malicious URL via the vulnerable GET parameter searchName", "searchValue", "searchDescription", "searchDefaultValue","searchPlugin", "searchDescription" and "searchDynamic" in the Server Properties and Security Audit Viewer JSP page	6.1	More Details
CVE-2020-12058	Several XSS vulnerabilities in osCommerce CE Phoenix before 1.0.6.0 allow an attacker to inject and execute arbitrary JavaScript code. The malicious code can be injected as follows: the page parameter to catalog/admin/order_status.php, catalog/admin/tax_rates.php, catalog/admin/languages.php, catalog/admin/countries.php, catalog/admin/tax_classes.php, catalog/admin/reviews.php, or catalog/admin/zones.php; or the zpage or spage parameter to catalog/admin/geo_zones.php.	6.1	More Details
CVE-2020-24601	In Ignite Realtime Openfire 4.5.1 a Stored Cross-site Vulnerability allows an attacker to execute an arbitrary malicious URL via the vulnerable POST parameter searchName", "alias" in the import certificate trusted page	6.1	More Details
CVE-2020-24553	Go before 1.14.8 and 1.15.x before 1.15.1 allows XSS because text/html is the default for CGI/FCGI handlers that lack a Content-Type header.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25093	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in blog.php. within application/views/templates/clothesshop, application/views/templates/onepage, and application/views/templates/redlabel.	6.1	More Details
CVE-2020-25092	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in _parts/header.php, within application/views/templates/clothesshop, application/views/templates/greenlabel, and application/views/templates/redlabel.	6.1	More Details
CVE-2019-11928	An input validation issue in WhatsApp Desktop versions prior to v0.3.4932 could have allowed cross-site scripting upon clicking on a link from a specially crafted live location message.	6.1	More Details
CVE-2020-25091	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/vendor/views/add_product.php.	6.1	More Details
CVE-2020-25088	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/admin/views/blog/blogpublish.php.	6.1	More Details
CVE-2020-25090	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/admin/views/ecommerce/publish.php.	6.1	More Details
CVE-2020-25089	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/admin/views/ecommerce/discounts.php.	6.1	More Details
CVE-2020-25086	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/admin/views/advanced_settings/adminUsers.php.	6.1	More Details
CVE-2020-25087	Ecommerce-CodeIgniter-Bootstrap before 2020-08-03 allows XSS in application/modules/admin/views/advanced_settings/languages.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3545	A vulnerability in Cisco FXOS Software could allow an authenticated, local attacker with administrative credentials to cause a buffer overflow condition. The vulnerability is due to incorrect bounds checking of values that are parsed from a specific file. An attacker could exploit this vulnerability by supplying a crafted file that, when it is processed, may cause a stack-based buffer overflow. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with root privileges. An attacker would need to have valid administrative credentials to exploit this vulnerability.	6.0	More Details
CVE-2020-7381	In Rapid7 Nexpose installer versions prior to 6.6.40, the Nexpose installer calls an executable which can be placed in the appropriate directory by an attacker with access to the local machine. This would prevent the installer from distinguishing between a valid executable called during a Security Console installation and any arbitrary code executable using the same file name.	5.8	More Details
CVE-2020-3537	A vulnerability in Cisco Jabber for Windows software could allow an authenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper validation of message contents. An attacker could exploit this vulnerability by sending specially crafted messages that contain Universal Naming Convention (UNC) links to a targeted user and convincing the user to follow the provided link. A successful exploit could allow the attacker to cause the application to access a remote system, possibly allowing the attacker to gain access to sensitive information that the attacker could use in additional attacks.	5.7	More Details
CVE-2020-3643	u'Information disclosure issue can occur due to partial secure display-touch session tear-down' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11122	u'Null Pointer exception while playing crafted mkv file as data stream get deleted on secondary invalid configuration' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8098, Bitra, Kamorta, SA6155P, Saipan, SM6150, SM7150, SM8150, SM8250, SXR2130	5.5	More Details
CVE-2020-16150	A Lucky 13 timing side channel in mbedtls_ssl_decrypt_buf in library/ssl_msg.c in Trusted Firmware Mbed TLS through 2.23.0 allows an attacker to recover secret key information. This affects CBC mode because of a computed time difference based on a padding length.	5.5	More Details
CVE-2020-15709	Versions of add-apt-repository before 0.98.9.2, 0.96.24.32.14, 0.96.20.10, and 0.92.37.8ubuntu0.1~esm1, printed a PPA (personal package archive) description to the terminal as-is, which allowed PPA owners to provide ANSI terminal escapes to modify terminal contents in unexpected ways.	5.5	More Details
CVE-2020-24385	In MidnightBSD before 1.2.6 and 1.3 before August 2020, and FreeBSD before 7, a NULL pointer dereference was found in the Linux emulation layer that allows attackers to crash the running kernel. During binary interaction, td->td_emuldata in sys/compat/linux/linux_emul.h is not getting initialized and returns NULL from em_find().	5.5	More Details
CVE-2020-10720	A flaw was found in the Linux kernel's implementation of GRO in versions before 5.2. This flaw allows an attacker with local access to crash the system.	5.5	More Details
CVE-2020-24863	A memory corruption vulnerability was found in the kernel function kern_getfsstat in MidnightBSD before 1.2.7 and 1.3 through 2020-08-19, and FreeBSD through 11.4, that allows an attacker to trigger an invalid free and crash the system via a crafted size value in conjunction with an invalid mode.	5.5	More Details
CVE-2020-3644	u'Information disclosure issue occurs as in current logic Secure Touch session is released without terminating display session' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14115	u'Information disclosure issue occurs as in current logic as secure touch is released without clearing the display session which can result in user reading the secure input while touch is in non-secure domain as secure display is active' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA515M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	5.5	More Details
CVE-2020-3620	u'Lack of check of integer overflow while doing a round up operation for data read from shared memory for G-link SMEM transport can lead to corruption and potential information leak' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3621	u'Lack of check to ensure that the TX read index & RX write index that are read from shared memory are less than the FIFO size results into memory corruption and potential information leakage' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SA415M, SA6155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	5.5	More Details
CVE-2019-14025	u'When a new session is created, Object is returned that contains TZ addresses and it get passed to HLOS as an handle to refer to a particular session and can cause TZ to jump to a invalid address' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130	5.5	More Details
CVE-2020-14373	A use after free was found in igc_reloc_struct_ptr() of psi/igc.c of ghostscript-9.25. A local attacker could supply a specially crafted PDF file to cause a denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9235	Huawei smartphones HONOR 20 PRO Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C185E3R5P1),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.212(C432E10R3P4),Versions earlier than 10.1.0.213(C636E3R4P3),Versions earlier than 10.1.0.214(C10E5R4P3),Versions earlier than 10.1.0.214(C185E3R3P3);Versions earlier than 10.1.0.212(C00E210R5P1);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C01E160R2P11);Versions earlier than 10.1.0.160(C00E160R2P11);Versions earlier than 10.1.0.160(C00E160R8P12);Versions earlier than 10.1.0.230(C432E9R5P1),Versions earlier than 10.1.0.231(C10E3R3P2),Versions earlier than 10.1.0.231(C636E3R3P1);Versions earlier than 10.1.0.225(C431E3R1P2),Versions earlier than 10.1.0.225(C432E3R1P2) contain an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerability to obtain some information. This can lead to information leak.	5.5	More Details
CVE-2020-4516	IBM Business Process Manager 8.5, 8.6 and IBM Business Automation Workflow 18.0, 19.0, and 20.0 are 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: 182371.	5.4	More Details
CVE-2020-4698	IBM Business Process Manager 8.5, 8.6 and IBM Business Automation Workflow 18.0, 19.0, and 20.0 are vulnerable to stored 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: 186841.	5.4	More Details
CVE-2020-24963	An Authenticated Persistent XSS vulnerability was discovered in the Best Support System, tested version v3.0.4.	5.4	More Details
CVE-2020-17458	A post-authenticated stored XSS was found in MultiUx v.3.1.12.0 via the /multiux/SaveMailbox LastName field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4702	IBM InfoSphere Information Server 11.7 is vulnerable to stored 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: 187187.	5.4	More Details
CVE-2020-4445	IBM Jazz Team Server based Applications are 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: 181122.	5.4	More Details
CVE-2020-4522	IBM Jazz Team Server based Applications are 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: 182397.	5.4	More Details
CVE-2020-4546	IBM Jazz Team Server based Applications are 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: 183314.	5.4	More Details
CVE-2020-8576	Clustered Data ONTAP versions prior to 9.3P19, 9.5P14, 9.6P9 and 9.7 are susceptible to a vulnerability which when successfully exploited could lead to addition or modification of data or disclosure of sensitive information.	5.4	More Details
CVE-2020-25104	eramba c2.8.1 and Enterprise before e2.19.3 allows XSS via a crafted filename for a file attached to an object. For example, the filename has a complete XSS payload followed by the .png extension.	5.4	More Details
CVE-2020-24981	An Incorrect Access Control vulnerability exists in /ucms/chk.php in UCMS 1.4.8. This results in information leak via an error message caused by directly accessing the website built by UCMS.	5.3	More Details
CVE-2020-25073	FreedomBox through 20.13 allows remote attackers to obtain sensitive information from the /server-status page of the Apache HTTP Server, because a connection from the Tor onion service (or from PageKite) is considered a local connection. This affects both the freedombox and plinth packages of some Linux distributions, but only if the Apache mod_status module is enabled.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3546	A vulnerability in the web-based management interface of Cisco AsyncOS software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to insufficient validation of requests that are sent to the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the interface of an affected device. A successful exploit could allow the attacker to obtain the IP addresses that are configured on the internal interfaces of the affected device. There is a workaround that addresses this vulnerability.	5.3	More Details
CVE-2020-3542	A vulnerability in Cisco Webex Training could allow an authenticated, remote attacker to join a password-protected meeting without providing the meeting password. The vulnerability is due to improper validation of input to API requests that are a part of meeting join flow. An attacker could exploit this vulnerability by sending an API request to the application, which would return a URL that includes a meeting join page that is prepopulated with the meeting username and password. A successful exploit could allow the attacker to join the password-protected meeting. The attacker would be visible in the attendee list of the meeting.	5.3	More Details
CVE-2020-7299	Cleartext Storage of Sensitive Information in Memory vulnerability in Microsoft Windows client in McAfee True Key (TK) prior to 6.2.109.2 allows a local user logged in with administrative privileges to access to another user's passwords on the same machine via triggering a process dump in specific situations.	5.0	More Details
CVE-2020-7119	A vulnerability exists in the Aruba Analytics and Location Engine (ALE) web management interface 2.1.0.2 and earlier firmware that allows an already authenticated administrative user to arbitrarily modify files as an underlying privileged operating system user.	4.9	More Details
CVE-2020-25116	The Admin CP in vBulletin 5.6.3 allows XSS via an Announcement Title to Channel Manager.	4.8	More Details
CVE-2020-25119	The Admin CP in vBulletin 5.6.3 allows XSS via a Title of a Child Help Item in the Login/Logoff part of the User Manual.	4.8	More Details
CVE-2020-25115	The Admin CP in vBulletin 5.6.3 allows XSS via an Occupation Title or Description to User Profile Field Manager.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25117	The Admin CP in vBulletin 5.6.3 allows XSS via a Junior Member Title to User Title Manager.	4.8	More Details
CVE-2020-25118	The Admin CP in vBulletin 5.6.3 allows XSS via a Style Options Settings Title to Styles Manager.	4.8	More Details
CVE-2020-25121	The Admin CP in vBulletin 5.6.3 allows XSS via the Paid Subscription Email Notification field in the Options.	4.8	More Details
CVE-2020-25120	The Admin CP in vBulletin 5.6.3 allows XSS via the admincp/search.php?do=dosearch URI.	4.8	More Details
CVE-2020-25123	The Admin CP in vBulletin 5.6.3 allows XSS via a Smilie Title to Smilies Manager.	4.8	More Details
CVE-2020-25124	The Admin CP in vBulletin 5.6.3 allows XSS via an admincp/attachment.php&do=rebuild&type= URI.	4.8	More Details
CVE-2020-25122	The Admin CP in vBulletin 5.6.3 allows XSS via a Rank Type to User Rank Manager.	4.8	More Details
CVE-2020-3453	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory.	4.7	More Details
CVE-2020-3451	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 Series Routers could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands on the underlying operating system (OS) as a restricted user. For more information about these vulnerabilities, see the Details section of this advisory.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3541	A vulnerability in the media engine component of Cisco Webex Meetings Client for Windows, Cisco Webex Meetings Desktop App for Windows, and Cisco Webex Teams for Windows could allow an authenticated, local attacker to gain access to sensitive information. The vulnerability is due to unsafe logging of authentication requests by the affected software. An attacker could exploit this vulnerability by reading log files that are stored in the application directory. A successful exploit could allow the attacker to gain access to sensitive information, which could be used in further attacks.	4.4	More Details
CVE-2020-3365	A vulnerability in the directory permissions of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker to perform a directory traversal attack on a limited set of restricted directories. The vulnerability is due to a flaw in the logic that governs directory permissions. An attacker could exploit this vulnerability by using capabilities that are not controlled by the role-based access control (RBAC) mechanisms of the software. A successful exploit could allow the attacker to overwrite files on an affected device.	4.3	More Details
CVE-2020-5418	Cloud Foundry CAPI (Cloud Controller) versions prior to 1.98.0 allow authenticated users having only the "cloud_controller.read" scope, but no roles in any spaces, to list all droplets in all spaces (whereas they should see none).	4.3	More Details
CVE-2020-3547	A vulnerability in the web-based management interface of Cisco AsyncOS software for Cisco Email Security Appliance (ESA), Cisco Content Security Management Appliance (SMA), and Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because an insecure method is used to mask certain passwords on the web-based management interface. An attacker could exploit this vulnerability by looking at the raw HTML code that is received from the interface. A successful exploit could allow the attacker to obtain some of the passwords configured throughout the interface.	4.3	More Details
CVE-2020-25026	The sf_event_mgt (aka Event management and registration) extension before 4.3.1 and 5.x before 5.1.1 for TYPO3 allows Information Disclosure (participant data, and event data via email) because of Broken Access Control.	4.3	More Details
CVE-2020-25025	The l10nmgr (aka Localization Manager) extension before 7.4.0, 8.x before 8.7.0, and 9.x before 9.2.0 for TYPO3 allows Information Disclosure (translatable fields).	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24654	In KDE Ark before 20.08.1, a crafted TAR archive with symlinks can install files outside the extraction directory, as demonstrated by a write operation to a user's home directory.	3.3	More Details
CVE-2020-9083	HUAWEI Mate 20 smart phones with Versions earlier than 10.1.0.163(C00E160R3P8) have a denial of service (DoS) vulnerability. The attacker can enter a large amount of text on the phone. Due to insufficient verification of the parameter, successful exploitation can impact the service.	2.4	More Details
CVE-2020-16149	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its requestor. Notes: none	N/A	More Details
CVE-2020-24979	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-24980	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details