SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 11 March 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-2020-9757	The SEOmatic component before 3.3.0 for Craft CMS allows Server-Side Template Injection that leads to RCE via malformed data to the metacontainers controller.	9.8	More Details
CVE-2020-10225	An unauthenticated file upload vulnerability has been identified in admin/gallery.php in PHPGurukul Job Portal 1.0. The vulnerability could be exploited by an unauthenticated remote attacker to upload content to the server, including PHP files, which could result in command execution.	9.8	More Details
CVE-2020-9761	An issue was discovered in UNCTAD ASYCUDA World 2001 through 2020. The Java RMI Server has an Insecure Default Configuration, leading to Java Code Execution from a remote URL because an RMI Distributed Garbage Collector method is called.	9.8	More Details
CVE-2020-9380	IPTV Smarters WEB TV PLAYER through 2020-02-22 allows attackers to execute OS commands by uploading a script.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10180	The ESET AV parsing engine allows virus-detection bypass via a crafted BZ2 Checksum field in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.	9.8	More Details
CVE-2019-17647	An issue was discovered in Centreon before 2.8.30, 18.10.8, 19.04.5, and 19.10.2. SQL Injection exists via the include/monitoring/status/Hosts/xml/hostXML.php instance parameter.	9.8	More Details
CVE-2020-10188	utility.c in telnetd in netkit telnet through 0.17 allows remote attackers to execute arbitrary code via short writes or urgent data, because of a buffer overflow involving the netclear and nextitem functions.	9.8	More Details
CVE-2020-10189	Zoho ManageEngine Desktop Central before 10.0.474 allows remote code execution because of deserialization of untrusted data in getChartImage in the FileStorage class. This is related to the CewolfServlet and MDMLogUploaderServlet servlets.	9.8	More Details
CVE-2020-8113	GitLab 10.7 and later through 12.7.2 has Incorrect Access Control.	9.8	More Details
CVE-2020-5328	Dell EMC Isilon OneFS versions prior to 8.2.0 contain an unauthorized access vulnerability due to a lack of thorough authorization checks when SyncIQ is licensed, but encrypted syncs are not marked as required. When this happens, loss of control of the cluster can occur.	9.8	More Details
CVE-2020-10212	upload.php in Responsive FileManager 9.13.4 and 9.14.0 allows SSRF via the url parameter because file-extension blocking is mishandled and because it is possible for a DNS hostname to resolve to an internal IP address. For example, an SSRF attempt may succeed if a .ico filename is added to the PATH_INFO. Also, an attacker could create a DNS hostname that resolves to the 0.0.0.0 IP address for DNS pinning. NOTE: this issue exists because of an incomplete fix for CVE-2018-14728.	9.8	More Details
CVE-2020-10220	An issue was discovered in rConfig through 3.9.4. The web interface is prone to a SQL injection via the commands.inc.php searchColumn parameter.	9.8	More Details
CVE-2020-10224	An unauthenticated file upload vulnerability has been identified in admin_add.php in PHPGurukul Online Book Store 1.0. The vulnerability could be exploited by an unauthenticated remote attacker to upload content to the server, including PHP files, which could result in command execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10232	In version 4.8.0 and earlier of The Sleuth Kit (TSK), there is a stack buffer overflow vulnerability in the YAFFS file timestamp parsing logic in yaffsfs_istat() in fs/yaffs.c.	9.8	More Details
CVE-2019-2317	The secret key used to make the Initial Sequence Number in the TCP SYN packet could be brute forced and therefore can be predicted in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, Nicobar, QCM2150, QM215, SC8180X, SDM429, SDM439, SDM450, SDM632, SDX24, SDX55, SM6150, SM7150, SM8150	9.8	More Details
CVE-2019-20504	service/krashrpt.php in Quest KACE K1000 Systems Management Appliance before 6.4 SP3 (6.4.120822) allows a remote attacker to execute code via shell metacharacters in the kuid parameter.	9.8	More Details
CVE-2014-1634	SQL Injection exists in Advanced Newsletter Magento extension before 2.3.5 via the /store/advancednewsletter/index/subscribeajax/an_category_id/ PATH_INFO.	9.8	More Details
CVE-2016-6918	Lexmark Markvision Enterprise (MVE) before 2.4.1 allows remote attackers to execute arbitrary commands by uploading files. (	9.8	More Details
CVE-2020-10250	BWA DiREX-Pro 1.2181 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the PKG parameter to uninstall.php3.	9.8	More Details
CVE-2020-10257	The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.	9.8	More Details
CVE-2017-10992	In HPE Storage Essentials 9.5.0.142, there is Unauthenticated Java Deserialization with remote code execution via OS commands in a request to invoker/JMXInvokerServlet, aka PSRT110461.	9.8	More Details
CVE-2018-14502	controllers/quizzes.php in the Kiboko Chained Quiz plugin before 1.0.9 for WordPress allows remote unauthenticated users to execute arbitrary SQL commands via the 'answer' and 'answers' parameters.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12428	An issue was discovered in GitLab Community and Enterprise Edition 6.8 through 11.11. Users could bypass the mandatory external authentication provider sign-in restrictions by sending a specially crafted request. It has Improper Authorization.	9.8	More Details
CVE-2019-12443	An issue was discovered in GitLab Community and Enterprise Edition 10.2 through 11.11. Multiple features contained Server-Side Request Forgery (SSRF) vulnerabilities caused by an insufficient validation to prevent DNS rebinding attacks.	9.8	More Details
CVE-2019-7589	A vulnerability with the SmartService API Service option exists whereby an unauthorized user could potentially exploit this to upload malicious code to the server that could be executed at system level privileges. This affects Johnson Controls' Kantech EntraPass Corporate Edition versions 8.0 and prior; Kantech EntraPass Global Edition versions 8.0 and prior.	9.8	More Details
CVE-2020-6198	SAP Solution Manager (Diagnostics Agent), version 720, allows unencrypted connections from unauthenticated sources. This allows an attacker to control all remote functions on the Agent due to Missing Authentication Check.	9.8	More Details
CVE-2020-10106	PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to SQL injection, as demonstrated by the email parameter in index.php or register.php. The SQL injection allows to dump the MySQL database and to bypass the login prompt.	9.8	More Details
CVE-2020-6207	SAP Solution Manager (User Experience Monitoring), version- 7.2, due to Missing Authentication Check does not perform any authentication for a service resulting in complete compromise of all SMDAgents connected to the Solution Manager.	9.8	More Details
CVE-2019-2311	Possible buffer overflow in WLAN handler due to lack of validation of destination buffer size before copying it 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, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996, MSM8996AU, MSM8998, QCA6174A, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9886, QCS605, SA6155P, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10594	Stack overflow can occur when SDP is received with multiple payload types in the FMTP attribute of a video M line in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, 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, QM215, Rennell, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2020-9477	An issue was discovered on HUMAX HGA12R-02 BRGCAA 1.1.53 devices. A vulnerability in the authentication functionality in the web-based interface could allow an unauthenticated remote attacker to capture packets at the time of authentication and gain access to the cleartext password. An attacker could use this access to create a new user account or control the device.	9.8	More Details
CVE-2020-9550	Rubetek SmartHome 2020 devices use unencrypted 433 MHz communication between controllers and beacons, allowing an attacker to sniff and spoof beacon requests remotely.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9054	Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2	9.8	More Details
CVE-2019-10526	Out of bound write in WLAN driver due to NULL character not properly placed after SSID name in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SC8180X, SDA845, SDM450, SDX20, SDX24, SDX55, SXR1130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10546	Buffer overflow can occur in WLAN firmware while parsing beacon/probe_response frames during roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8096, APQ8096AU, IPQ6018, IPQ8074, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCS404, QCS605, Rennell, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.8	More Details
CVE-2019-2300	Possible buffer overflow in WLAN handler due to lack of validation of destination buffer size before copying into it 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, APQ8096, APQ8098, IPQ8074, MDM9206, MDM9207C, MDM9607, MSM8996, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCA9886, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2019-10587	Possible Stack overflow can occur when processing a large SDP body or non standard SDP body without right delimiters in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, 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, QM215, Rennell, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10593	Buffer overflow can occur when processing non standard SDP video Image attribute parameter in a VILTE\VOLTE call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2019-10586	Filling media attribute tag names without validating the destination buffer size which can result in the buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2019-10612	UTCB object has a function pointer called by the reaper to deallocate its memory resources and this address can potentially be corrupted by stack overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, MDM9650, QCS605, SA6155P, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14083	While parsing Service Descriptor Extended Attribute received as part of SDF frame, there is a possibility that incorrect length is specified in the attribute length field of extended SSI which can lead to integer underflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8096, APQ8098, IPQ6018, IPQ8074, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS404, QCS405, QCS605, Rennell, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130, SXR2130	9.8	More Details
CVE-2019-14045	Possible buffer overflow while processing clientlog and serverlog due to lack of validation of data received in logs in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8096AU, QCS605, SDM439, SM8150, SXR1130	9.8	More Details
CVE-2019-14098	Possible buffer overflow in data offload handler due to lack of check of keydata length when copying data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096, APQ8096AU, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA4531, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA9377, QCA9379, QCA9886, QCS405, QCS605, Rennell, SA6155P, SC8180X, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130, SXR2130	9.8	More Details
CVE-2019-14097	Possible buffer overflow in WLAN Parser due to lack of length check when copying data 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 APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, Rennell, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14095	Buffer overflow occurs while processing LMP packet in which name length parameter exceeds value specified in BT-specification in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8016, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9379, QCA9886, QCM2150, QCN7605, QCS404, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.8	More Details
CVE-2019-14086	Possible integer overflow while checking the length of frame which is a 32 bit integer and is added to another 32 bit integer which can lead to unexpected result during the check in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, MDM9607, MSM8998, QCA6584, QCN7605, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2019-14031	Buffer overflow can occur while parsing RSN IE containing list of PMK ID`s which are more than the buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA4531, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9886, QCN7605, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9758	An issue was discovered in chat.php in LiveZilla Live Chat 8.0.1.3 (Helpdesk). A blind JavaScript injection lies in the name parameter. Triggering this can fetch the username and passwords of the helpdesk employees in the URI. This leads to a privilege escalation, from unauthenticated to user-level access, leading to full account takeover. The attack fetches multiple credentials because they are stored in the database (stored XSS). This affects the mobile/chat URI via the lgn and psswrd parameters.	9.6	More Details
CVE-2020-6203	SAP NetWeaver UDDI Server (Services Registry), versions- 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; allows an attacker to exploit insufficient validation of path information provided by users, thus characters representing 'traverse to parent directory' are passed through to the file APIs, leading to Path Traversal.	9.1	More Details
CVE-2019-10552	Multiple Buffer Over-read issue can happen due to improper length checks while decoding Service Reject/RAU Reject/PTMSI Realloc cmd in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details
CVE-2019-10550	Buffer Over-read when UE is trying to process the message received form the network without zero termination in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS605, QM215, Rennell, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10553	Multiple Read overflows due to improper length checks while decoding authentication in Cs domain/RAU Reject and TC cmd in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details
CVE-2019-10554	Multiple Read overflows issue due to improper length check while decoding Identity Request in CSdomain/Authentication Reject in CS domain/ PRAU accept/while logging DL message in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details
CVE-2019-10577	Improper input validation while processing SIP URI received from the network will lead to buffer over-read and then to denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14082	Potential buffer over-read due to lack of bound check of memory offset passed in WLAN firmware in Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9207C, MDM9607, QCN7605, SM8150	9.1	More Details
CVE-2020-10233	In version 4.8.0 and earlier of The Sleuth Kit (TSK), there is a heap-based buffer over-read in ntfs_dinode_lookup in fs/ntfs.c.	9.1	More Details
CVE-2020-9370	HUMAX HGA12R-02 BRGCAA 1.1.53 devices allow Session Hijacking.	9.1	More Details
CVE-2020-10255	Modern DRAM chips (DDR4 and LPDDR4 after 2015) are affected by a vulnerability in deployment of internal mitigations against RowHammer attacks known as Target Row Refresh (TRR), aka the TRRespass issue. To exploit this vulnerability, the attacker needs to create certain access patterns to trigger bit flips on affected memory modules, aka a Many-sided RowHammer attack. This means that, even when chips advertised as RowHammer-free are used, attackers may still be able to conduct privilege-escalation attacks against the kernel, conduct privilege-escalation attacks against the Sudo binary, and achieve cross-tenant virtual-machine access by corrupting RSA keys. The issue affects chips produced by SK Hynix, Micron, and Samsung. NOTE: tracking DRAM supply-chain issues is not straightforward because a single product model from a single vendor may use DRAM chips from different manufacturers.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-5535	OpenBlocks IoT VX2 prior to Ver.4.0.0 (Ver.3 Series) allows an attacker on the same network segment to execute arbitrary OS commands with root privileges via unspecified vectors.	8.8	More Details
CVE-2020-10190	An issue was discovered in MunkiReport before 5.3.0. An authenticated user could achieve SQL Injection in app/models/tablequery.php by crafting a special payload on the /datatables/data endpoint.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10216	An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the date parameter in a system_time.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.	8.8	More Details
CVE-2020-10215	An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the dns_query_name parameter in a dns_query.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.	8.8	More Details
CVE-2020-10214	An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. There is a stack-based buffer overflow in the httpd binary. It allows an authenticated user to execute arbitrary code via a POST to ntp_sync.cgi with a sufficiently long parameter ntp_server.	8.8	More Details
CVE-2020-10213	An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the wps_sta_enrollee_pin parameter in a set_sta_enrollee_pin.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.	8.8	More Details
CVE-2019-9859	Vesta Control Panel (VestaCP) 0.9.7 through 0.9.8-23 is vulnerable to an authenticated command execution that can result in remote root access on the server. The platform works with PHP as the frontend language and uses shell scripts to execute system actions. PHP executes shell script through the dangerous command exec. This function can be dangerous if arguments passed to it are not filtered. Every user input in VestaCP that is used as an argument is filtered with the escapeshellarg function. This function comes from the PHP library directly and its description is as follows: "escapeshellarg() adds single quotes around a string and quotes/escapes any existing single quotes allowing you to pass a string directly to a shell function and having it be treated as a single safe argument." It means that if you give Username, it will have 'Username' as a replacement. This works well and protects users from exploiting this potentially dangerous exec function. Unfortunately, VestaCP uses this escapeshellarg function incorrectly in several places.	8.8	More Details
CVE-2019-12430	An issue was discovered in GitLab Community and Enterprise Edition 11.11. A specially crafted payload would allow an authenticated malicious user to execute commands remotely through the repository download feature. It allows Command Injection.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19292	A vulnerability has been identified in Control Center Server (CCS) (All versions < V1.5.0). The Control Center Server (CCS) contains an SQL injection vulnerability in its XML-based communication protocol as provided by default on ports 5444/tcp and 5440/tcp. An authenticated remote attacker could exploit this vulnerability to read or modify the CCS database and potentially execute administrative database operations or operating system commands.	8.8	More Details
CVE-2020-9458	In the RegistrationMagic plugin through 4.6.0.3 for WordPress, the export function allows remote authenticated users (with minimal privileges) to export submitted form data and settings via class_rm_form_controller.php rm_form_export.	8.8	More Details
CVE-2020-9457	The RegistrationMagic plugin through 4.6.0.3 for WordPress allows remote authenticated users (with minimal privileges) to import custom vulnerable forms and change form settings via class_rm_form_settings_controller.php, resulting in privilege escalation.	8.8	More Details
CVE-2020-9456	In the RegistrationMagic plugin through 4.6.0.3 for WordPress, the user controller allows remote authenticated users (with minimal privileges) to elevate their privileges to administrator via class_rm_user_controller.php rm_user_edit.	8.8	More Details
CVE-2020-9454	A CSRF vulnerability in the RegistrationMagic plugin through 4.6.0.3 for WordPress allows remote attackers to forge requests on behalf of a site administrator to change all settings for the plugin, including deleting users, creating new roles with escalated privileges, and allowing PHP file uploads via forms.	8.8	More Details
CVE-2019-20107	Multiple SQL injection vulnerabilities in TestLink through 1.9.19 allows remote authenticated users to execute arbitrary SQL commands via the (1) tproject_id parameter to keywordsView.php; the (2) req_spec_id parameter to reqSpecCompareRevisions.php; the (3) requirement_id parameter to reqCompareVersions.php; the (4) build_id parameter to planUpdateTC.php; the (5) tplan_id parameter to newest_tcversions.php; the (6) tplan_id parameter to tcCreatedPerUserGUI.php; the (7) tcase_id parameter to tcAssign2Tplan.php; or the (8) testcase_id parameter to tcCompareVersions.php. Authentication is often easy to achieve: a guest account, that can execute this attack, can be created by anyone in the default configuration.	8.8	More Details
CVE-2020-10173	Comtrend VR-3033 DE11-416SSG-C01_R02.A2pvl042j1.d26m devices have Multiple Authenticated Command Injection vulnerabilities via the ping and traceroute diagnostic pages, as demonstrated by shell metacharacters in the pingIpAddress parameter to ping.cgi.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9402	Django 1.11 before 1.11.29, 2.2 before 2.2.11, and 3.0 before 3.0.4 allows SQL Injection if untrusted data is used as a tolerance parameter in GIS functions and aggregates on Oracle. By passing a suitably crafted tolerance to GIS functions and aggregates on Oracle, it was possible to break escaping and inject malicious SQL.	8.8	More Details
CVE-2020-0032	In ih264d_release_display_bufs of ih264d_utils.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-145364230	8.8	More Details
CVE-2020-10221	lib/ajaxHandlers/ajaxAddTemplate.php in rConfig through 3.94 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the fileName POST parameter.	8.8	More Details
CVE-2019-17642	An issue was discovered in Centreon before 18.10.8, 19.10.1, and 19.04.2. It allows CSRF with resultant remote command execution via shell metacharacters in a POST to centreon-autodiscovery-server/views/scan/ajax/call.php in the Autodiscovery plugin.	8.8	More Details
CVE-2020-2134	Sandbox protection in Jenkins Script Security Plugin 1.70 and earlier could be circumvented through crafted constructor calls and crafted constructor bodies.	8.8	More Details
CVE-2020-2158	Jenkins Literate Plugin 1.0 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	8.8	More Details
CVE-2020-10057	GeniXCMS 1.1.7 is vulnerable to user privilege escalation due to broken access control. This issue exists because of an incomplete fix for CVE-2015-2680, in which "token" is used as a CSRF protection mechanism, but without validation that "token" is associated with an administrative user.	8.8	More Details
CVE-2020-2135	Sandbox protection in Jenkins Script Security Plugin 1.70 and earlier could be circumvented through crafted method calls on objects that implement GroovyInterceptable.	8.8	More Details
CVE-2015-7339	JCE Joomla Component 2.5.0 to 2.5.2 allows arbitrary file upload via a .php file extension for an image file to the /com_jce/editor/libraries/classes/browser.php script.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10235	An issue was discovered in Froxlor before 0.10.14. Remote attackers with access to the installation routine could have executed arbitrary code via the database configuration options that were passed unescaped to exec, because of _backupExistingDatabase in install/lib/class.FroxlorInstall.php.	8.8	More Details
CVE-2015-7341	JNews Joomla Component before 8.5.0 allows arbitrary File Upload via Subscribers or Templates, as demonstrated by the .php5 extension.	8.8	More Details
CVE-2020-2159	Jenkins CryptoMove Plugin 0.1.33 and earlier allows attackers with Job/Configure access to execute arbitrary OS commands on the Jenkins master as the OS user account running Jenkins.	8.8	More Details
CVE-2020-5536	OpenBlocks IoT VX2 prior to Ver.4.0.0 (Ver.3 Series) allows an attacker on the same network segment to bypass authentication and to initialize the device via unspecified vectors.	8.8	More Details
CVE-2016-1487	Lexmark Markvision Enterprise before 2.3.0 misuses the Apache Commons Collections Library, leading to remote code execution because of Java deserialization.	8.8	More Details
CVE-2020-7988	An issue was discovered in tools/pass-change/result.php in phpIPAM 1.4. CSRF can be used to change the password of any user/admin, to escalate privileges, and to gain access to more data and functionality. This issue exists due to the lack of a requirement to provide the old password, and the lack of security tokens.	8.8	More Details
CVE-2020-10185	The sync endpoint in YubiKey Validation Server before 2.40 allows remote attackers to replay an OTP. NOTE: this issue is potentially relevant to persons outside Yubico who operate a self-hosted OTP validation service with a non-default configuration such as an open sync pool; the issue does NOT affect YubiCloud.	8.6	More Details
CVE-2020-6208	SAP Business Objects Business Intelligence Platform (Crystal Reports), versions- 4.1, 4.2, allows an attacker with basic authorization to inject code that can be executed by the application and thus allowing the attacker to control the behaviour of the application, leading to Remote Code Execution. Although the mode of attack is only Local, multiple applications can be impacted as a result of the vulnerability.	8.2	More Details
CVE-2020-10222	npdf.dll in Nitro Pro before 13.13.2.242 is vulnerable to Heap Corruption at npdf!nitro::get_property+2381 via a crafted PDF document.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10223	npdf.dll in Nitro Pro before 13.13.2.242 is vulnerable to JBIG2Decode CNxJBIG2DecodeStream Heap Corruption at npdf!CAPPDAnnotHandlerUtils::create_popup_for_markup+0x12fbe via a crafted PDF document.	8.1	More Details
CVE-2020-5327	Dell Security Management Server versions prior to 10.2.10 contain a Java RMI Deserialization of Untrusted Data vulnerability. When the server is exposed to the internet and Windows Firewall is disabled, a remote unauthenticated attacker may exploit this vulnerability by sending a crafted RMI request to execute arbitrary code on the target host.	8.1	More Details
CVE-2019-17636	In Eclipse Theia versions 0.3.9 through 0.15.0, one of the default pre-packaged Theia extensions is "Mini-Browser", published as "@theia/mini-browser" on npmjs.com. This extension, for its own needs, exposes a HTTP endpoint that allows to read the content of files on the host's filesystem, given their path, without restrictions on the requester's origin. This design is vulnerable to being exploited remotely through a DNS rebinding attack or a drive-by download of a carefully crafted exploit.	8.1	More Details
CVE-2020-5256	BookStack before version 0.25.5 has a vulnerability where a user could upload PHP files through image upload functions, which would allow them to execute code on the host system remotely. They would then have the permissions of the PHP process. This most impacts scenarios where non-trusted users are given permission to upload images in any area of the application. The issue was addressed in a series of patches in versions 0.25.3, 0.25.4 and 0.25.5. Users should upgrade to at least v0.25.5 to avoid this vulnerability.	7.9	More Details
CVE-2019-14027	Buffer overflow due to lack of upper bound check on channel length which is used for a loop. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ6018, IPQ8074, MSM8998, Nicobar, QCA8081, QCN7605, QCS404, QCS605, Rennell, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130	7.8	More Details
CVE-2019-14068	Out of bound access in msm routing due to lack of check of size before accessing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8096AU, MDM9607, MSM8905, MSM8909W, Nicobar, QCS405, QCS605, Rennell, Saipan, SDM429W, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14029	Use-after-free in graphics module due to destroying already queued syncobj in error case in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MDM9607, MSM8909W, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-14030	The size of a buffer is determined by addition and multiplications operations that have the potential to overflow due to lack of bound check in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, Rennell, SC8180X, SDM845, SDM850, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2019-14032	Memory use after free issue in audio due to lack of resource control in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, Rennell, SA6155P, Saipan, SC8180X, SDA845, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-14048	Possible out of bound memory access while playing a crafted clip in media player in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in SM8150	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14050	Out-of-bound writes occurs due to lack of check of buffer size will cause buffer overflow only in 32bit architecture. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, MDM9150, MDM9205, MDM9607, MDM9650, MSM8905, Nicobar, QCS405, QCS605, Rennell, SA6155P, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130	7.8	More Details
CVE-2020-9756	Patriot Viper RGB Driver 1.1 and prior exposes IOCTL and allows insufficient access control. The IOCTL Codes 0x80102050 and 0x80102054 allows a local user with low privileges to read/write 1/2/4 bytes from or to an IO port. This could be leveraged in a number of ways to ultimately run code with elevated privileges.	7.8	More Details
CVE-2020-4278	IBM Platform LSF 9.1 and 10.1, IBM Spectrum LSF Suite 10.2, and IBM Spectrum Suite for HPA 10.2 could allow a local user to escalate their privileges due to weak file permissions when specific debug settings are enabled in a Linux or Unix enviornment. IBM X-Force ID: 176137.	7.8	More Details
CVE-2020-0033	In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds write due to stale pointer. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144351324	7.8	More Details
CVE-2019-14085	Possible Integer underflow in WLAN function due to lack of check of data received from user side in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCN7605, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SM8150, SXR1130	7.8	More Details
CVE-2019-20501	D-Link DWL-2600AP 4.2.0.15 Rev A devices have an authenticated OS command injection vulnerability via the Upgrade Firmware functionality in the Web interface, using shell metacharacters in the admin.cgi? action=upgrade firmwareRestore or firmwareServerip parameter.	7.8	More Details
CVE-2019-20500	D-Link DWL-2600AP 4.2.0.15 Rev A devices have an authenticated OS command injection vulnerability via the Save Configuration functionality in the Web interface, using shell metacharacters in the admin.cgi? action=config_save configBackup or downloadServerip parameter.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14071	Compromised reset handler may bypass access control due to AC config is being reset if debug path is enabled to collect secure or non-secure ram dumps in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ6018, MDM9205, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QM215, Rennell, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	7.8	More Details
CVE-2019-20499	D-Link DWL-2600AP 4.2.0.15 Rev A devices have an authenticated OS command injection vulnerability via the Restore Configuration functionality in the Web interface, using shell metacharacters in the admin.cgi? action=config_restore configRestore or configServerip parameter.	7.8	More Details
CVE-2020-5957	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges.	7.8	More Details
CVE-2019-14079	Access to the uninitialized variable when the driver tries to unmap the dma buffer of a request which was never mapped in the first place leading to kernel failure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MDM9607, MDM9640, MSM8909W, MSM8953, QCA6574AU, QCS605, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SM8150, SXR1130	7.8	More Details
CVE-2020-6971	In Emerson ValveLink v12.0.264 to v13.4.118, a vulnerability in the ValveLink software may allow a local, unprivileged, trusted insider to escalate privileges due to insecure configuration parameters.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14028	Buffer overwrite during memcpy due to lack of check on SSID length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, Nicobar, QCA4531, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9886, QCN7605, QCS404, QCS405, QCS605, Rennell, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-0084	In several functions of NotificationManagerService.java, there are missing permission checks. This could lead to local escalation of privilege by creating fake system notifications with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143339775	7.8	More Details
CVE-2019-14026	Possible buffer overflow in WLAN WMI handler due to lack of ssid length check when copying data 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, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574, QCA6574AU, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9886, QCN7605, QCS404, QCS405, QCS605, Rennell, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-14015	A stack-based buffer overflow exists in the initialization of the identification stage due to lack of check on the number of templates provided. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096, APQ8096AU, MDM9205, MSM8996, MSM8996AU, Nicobar, QCS404, QCS405, QCS605, Rennell, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0054	In WifiNetworkSuggestionsManager of WifiNetworkSuggestionsManager.java, there is a possible permission revocation due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146642727	7.8	More Details
CVE-2020-0051	In onCreate of SettingsHomepageActivity, there is a possible tapjacking attack. This could lead to local escalation of privilege in Settings with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-138442483	7.8	More Details
CVE-2020-9470	An issue was discovered in Wing FTP Server 6.2.5 before February 2020. Due to insecure permissions when handling session cookies, a local user may view the contents of the session and session_admin directories, which expose active session cookies within the Wing FTP HTTP interface and administration panel. These cookies may be used to hijack user and administrative sessions, including the ability to execute Lua commands as root within the administration panel.	7.8	More Details
CVE-2020-5342	Dell Digital Delivery versions prior to 3.5.2015 contain an incorrect default permissions vulnerability. A locally authenticated low-privileged malicious user could exploit this vulnerability to run an arbitrary executable with administrative privileges on the affected system.	7.8	More Details
CVE-2020-9372	The Appointment Booking Calendar plugin before 1.3.35 for WordPress allows user input (in fields such as Description or Name) in any booking form to be any formula, which then could be exported via the Bookings list tab in /wp-admin/admin.php?page=cpabc_appointments.php. The attacker could achieve remote code execution via CSV injection.	7.8	More Details
CVE-2020-3128	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3127	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	7.8	More Details
CVE-2020-0046	In DrmPlugin::releaseSecureStops of DrmPlugin.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-137284652	7.8	More Details
CVE-2020-8635	Wing FTP Server v6.2.3 for Linux, macOS, and Solaris sets insecure permissions on installation directories and configuration files. This allows local users to arbitrarily create FTP users with full privileges, and escalate privileges within the operating system by modifying system files.	7.8	More Details
CVE-2020-8634	Wing FTP Server v6.2.3 for Linux, macOS, and Solaris sets insecure permissions on files modified within the HTTP file management interface, resulting in files being saved with world-readable and world-writable permissions. If a sensitive system file were edited this way, a low-privilege user may escalate privileges to root.	7.8	More Details
CVE-2020-0069	In the ioctl handlers of the Mediatek Command Queue driver, there is a possible out of bounds write due to insufficient input sanitization and missing SELinux restrictions. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-147882143References: M-ALPS04356754	7.8	More Details
CVE-2020-9418	An untrusted search path vulnerability in the installer of PDFescape Desktop version 4.0.22 and earlier allows an attacker to gain privileges and execute code via DLL hijacking.	7.8	More Details
CVE-2020-0041	In binder_transaction of binder.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-145988638References: Upstream kernel	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-11838	Possible double free issue in WLAN due to lack of checking memory free condition. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, MDM9640, SDA660, SDM636, SDM660, SDX20	7.8	More Details
CVE-2019-10569	Stack buffer overflow due to instance id is misplaced inside definition of hardware accelerated effects in makefile in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile in APQ8053, APQ8098, MDM9607, MDM9640, MSM8998, QCS605, SC8180X, SDM439, SDM630, SDM636, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	7.8	More Details
CVE-2020-0085	In setBluetoothTethering of PanService.java, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege to activate tethering with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-134487438	7.8	More Details
CVE-2019-10603	Use after free issue occurs If the real device interface goes down and a route lookup is performed while sending a raw IPv6 message in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8937, MSM8996AU, QCN7605, SDA845, SDM630, SDM636, SDM660, SDX20, SXR1130	7.8	More Details
CVE-2019-10604	Possibility of heap-buffer-overflow during last iteration of loop while populating image version information in diag command response packet, in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MDM9607, MDM9640, MSM8909W, MSM8917, MSM8953, Nicobar, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-0036	In hasPermissions of PermissionMonitor.java, there is a possible access to restricted permissions due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144679405	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14000	Lack of check that the RX FIFO write index that is read from shared RAM is less than the FIFO size results into memory corruption and potential information leakage 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, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9607, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCS404, QCS405, QCS605, QM215, Rennell, SA6155P, 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-2020-5259	In affected versions of dojox (NPM package), the jqMix method is vulnerable to Prototype Pollution. Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects. An attacker manipulates these attributes to overwrite, or pollute, a JavaScript application object prototype of the base object by injecting other values. This has been patched in versions 1.11.10, 1.12.8, 1.13.7, 1.14.6, 1.15.3 and 1.16.2	7.7	More Details
CVE-2020-5251	In parser-server before version 4.1.0, you can fetch all the users objects, by using regex in the NoSQL query. Using the NoSQL, you can use a regex on sessionToken and find valid accounts this way.	7.7	More Details
CVE-2020-5258	In affected versions of dojo (NPM package), the deepCopy method is vulnerable to Prototype Pollution. Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects. An attacker manipulates these attributes to overwrite, or pollute, a JavaScript application object prototype of the base object by injecting other values. This has been patched in versions 1.12.8, 1.13.7, 1.14.6, 1.15.3 and 1.16.2	7.7	More Details
CVE-2020-5250	In PrestaShop before version 1.7.6.4, when a customer edits their address, they can freely change the id_address in the form, and thus steal someone else's address. It is the same with CustomerForm, you are able to change the id_customer and change all information of all accounts. The problem is patched in version 1.7.6.4.	7.6	More Details
CVE-2019-12446	An issue was discovered in GitLab Community and Enterprise Edition 8.3 through 11.11. It allows Information Exposure through an Error Message.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10096	An issue was discovered in Zammad 3.0 through 3.2. It does not prevent caching of confidential data within browser memory. An attacker who either remotely compromises or obtains physical access to a user's workstation can browse the browser cache contents and obtain sensitive information. The attacker does not need to be authenticated with the application to view this information, as it would be available via the browser cache.	7.5	More Details
CVE-2019-19279	A vulnerability has been identified in SIPROTEC 4 and SIPROTEC Compact relays equipped with EN100 Ethernet communication modules (All versions). Specially crafted packets sent to port 50000/UDP of the EN100 Ethernet communication modules could cause a Denial-of-Service of the affected device. A manual reboot is required to recover the service of the device. At the time of advisory publication no public exploitation of this security vulnerability was known to Siemens.	7.5	More Details
CVE-2011-3269	Lexmark X, W, T, E, C, 6500e, and 25xxN devices before 2011-11-15 allow attackers to obtain sensitive information via a hidden email address in a Scan To Email shortcut.	7.5	More Details
CVE-2019-18336	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V3.X.17), SIMATIC TDC CP51M1 (All versions < V1.1.8), SIMATIC TDC CPU555 (All versions < V1.1.1), SINUMERIK 840D sl (All versions < V4.8.6), SINUMERIK 840D sl (All versions < V4.94). Specially crafted packets sent to port 102/tcp (Profinet) could cause the affected device to go into defect mode. A restart is required in order to recover the system. Successful exploitation requires an attacker to have network access to port 102/tcp, with no authentication. No user interation is required. At the time of advisory publication no public exploitation of this security vulnerability was known.	7.5	More Details
CVE-2020-0083	In setRequirePmfInternal of sta_network.cpp, there is a possible default value being improperly applied due to a logic error. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142797954	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9044	XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.	7.5	More Details
CVE-2019-13121	An issue was discovered in GitLab Enterprise Edition 10.6 through 12.0.2. The GitHub project integration was vulnerable to an SSRF vulnerability which allowed an attacker to make requests to local network resources. It has Incorrect Access Control.	7.5	More Details
CVE-2019-19225	A Broken Access Control vulnerability in the D-Link DSL-2680 web administration interface (Firmware EU_1.03) allows an attacker to change DNS servers without being authenticated on the admin interface by submitting a crafted Forms/dns_1 POST request.	7.5	More Details
CVE-2012-1094	JBoss AS 7 prior to 7.1.1 and mod_cluster do not handle default hostname in the same way, which can cause the excluded-contexts list to be mismatched and the root context to be exposed.	7.5	More Details
CVE-2019-11938	Java Facebook Thrift servers would not error upon receiving messages declaring containers of sizes larger than the payload. As a result, malicious clients could send short messages which would result in a large memory allocation, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.12.09.00.	7.5	More Details
CVE-2019-13003	An issue was discovered in GitLab Community and Enterprise Edition before 12.0.3. One of the parsers used by Gilab CI was vulnerable to a resource exhaustion attack. It allows Uncontrolled Resource Consumption.	7.5	More Details
CVE-2019-17645	An issue was discovered in Centreon before 2.8.31, 18.10.9, 19.04.6, and 19.10.3. It provides sensitive information via an unauthenticated direct request for include/configuration/configObject/service/refreshMacroAjax.php.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12441	An issue was discovered in GitLab Community and Enterprise Edition 8.4 through 11.11. The protected branches feature contained a access control issue which resulted in a bypass of the protected branches restriction rules. It has Incorrect Access Control.	7.5	More Details
CVE-2019-10705	Western Digital SanDisk X600 devices in certain configurations, a vulnerability in the access control mechanism of the drive may allow data to be decrypted without knowledge of proper authentication credentials.	7.5	More Details
CVE-2020-1737	A flaw was found in Ansible 2.7.17 and prior, 2.8.9 and prior, and 2.9.6 and prior when using the Extract-Zip function from the win_unzip module as the extracted file(s) are not checked if they belong to the destination folder. An attacker could take advantage of this flaw by crafting an archive anywhere in the file system, using a path traversal. This issue is fixed in 2.10.	7.5	More Details
CVE-2019-19282	A vulnerability has been identified in OpenPCS 7 V8.1 (All versions), OpenPCS 7 V8.2 (All versions), OpenPCS 7 V9.0 (All versions < V9.0 Upd3), SIMATIC BATCH V8.1 (All versions), SIMATIC BATCH V8.2 (All versions < V8.2 Upd12), SIMATIC BATCH V9.0 (All versions < V9.0 SP1 Upd5), SIMATIC NET PC Software V14 (All versions < V14 SP1 Update 14), SIMATIC NET PC Software V15 (All versions), SIMATIC NET PC Software V16 (All versions < V16 Update 1), SIMATIC PCS 7 V8.1 (All versions), SIMATIC PCS 7 V8.2 (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC Route Control V8.1 (All versions), SIMATIC Route Control V8.2 (All versions), SIMATIC Route Control V9.0 (All versions < V9.0 Upd4), SIMATIC WinCC (TIA Portal) V13 (All versions < V13 SP2), SIMATIC WinCC (TIA Portal) V14 (All versions < V14 SP1 Update 10), SIMATIC WinCC (TIA Portal) V15.1 (All versions < V15.1 Update 5), SIMATIC WinCC (TIA Portal) V16 (All versions < V16 Update 1), SIMATIC WinCC V7.3 (All versions), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 1). Through specially crafted messages, when encrypted communication is enabled, an attacker with network access could use the vulnerability to compromise the availability of the system by causing a Denial-of-Service condition. Successful exploitation requires no system privileges and no user interaction.	7.5	More Details
CVE-2019-3553	C++ Facebook Thrift servers would not error upon receiving messages declaring containers of sizes larger than the payload. As a result, malicious clients could send short messages which would result in a large memory allocation, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2020.02.03.00.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-18894	Certain older Lexmark devices (C, M, X, and 6500e before 2018-12-18) contain a directory traversal vulnerability in the embedded web server.	7.5	More Details
CVE-2019-17644	An issue was discovered in Centreon before 2.8-30, 18.10-8, 19.04-5, and 19.10-2.. It provides sensitive information via an unauthenticated direct request for include/configuration/configObject/host/refreshMacroAjax.php.	7.5	More Details
CVE-2019-17643	An issue was discovered in Centreon before 2.8-30,18.10-8, 19.04-5, and 19.10-2. It provides sensitive information via an unauthenticated direct request for include/monitoring/recurrentDowntime/GetXMLHost4Services.php.	7.5	More Details
CVE-2020-8661	CNCF Envoy through 1.13.0 may consume excessive amounts of memory when responding internally to pipelined requests.	7.5	More Details
CVE-2020-8659	CNCF Envoy through 1.13.0 may consume excessive amounts of memory when proxying HTTP/1.1 requests or responses with many small (i.e. 1 byte) chunks.	7.5	More Details
CVE-2020-7130	HPE OneView Global Dashboard (OVGD) 1.9 has a remote information disclosure vulnerability. HPE OneView Global Dashboard - After Upgrade or Install of OVGD Version 1.9, Appliance Firewall May Leave Ports Open. This is resolved in OVGD 1.91 or later.	7.5	More Details
CVE-2020-9476	ARRIS TG1692A devices allow remote attackers to discover the administrator login name and password by reading the /login page and performing base64 decoding.	7.5	More Details
CVE-2019-19226	A Broken Access Control vulnerability in the D-Link DSL-2680 web administration interface (Firmware EU_1.03) allows an attacker to enable or disable MAC address filtering by submitting a crafted Forms/WlanMacFilter_1 POST request without being authenticated on the admin interface.	7.5	More Details
CVE-2020-10248	BWA DiREX-Pro 1.2181 devices allow remote attackers to discover passwords via a direct request to val_users.php3.	7.5	More Details
CVE-2020-0062	In Euicc, there is a possible information disclosure due to an included test Certificate. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-143232031	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10244	JPaseto before 0.3.0 generates weak hashes when using v2.local tokens.	7.5	More Details
CVE-2019-19614	An issue was discovered in Halvotec RAQuest 10.23.10801.0. The login page is vulnerable to wildcard injection, allowing an attacker to enumerate the list of users sharing an identical password. Fixed in Release 10.24.11206.1.	7.5	More Details
CVE-2019-19281	A vulnerability has been identified in SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions >= V2.5 and < V20.8), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions >= V2.5 and < V2.8), SIMATIC S7-1500 Software Controller (All versions >= V2.5 and < V20.8). Affected devices contain a vulnerability that allows an unauthenticated attacker to trigger a Denial-of-Service condition. The vulnerability can be triggered if specially crafted UDP packets are sent to the device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the device availability.	7.5	More Details
CVE-2019-19224	A Broken Access Control vulnerability in the D-Link DSL-2680 web administration interface (Firmware EU_1.03) allows an attacker to download the configuration (binary file) settings by submitting a rom-0 GET request without being authenticated on the admin interface.	7.5	More Details
CVE-2020-10101	An issue was discovered in Zammad 3.0 through 3.2. The WebSocket server crashes when messages in non-JSON format are sent by an attacker. The message format is not properly checked and parsing errors not handled. This leads to a crash of the service process.	7.5	More Details
CVE-2019-19298	A vulnerability has been identified in SiNVR/SiVMS Video Server (All versions < V5.0.0), SiNVR/SiVMS Video Server (All versions >= V5.0.0 < V5.0.2). The streaming service (default port 5410/tcp) of the SiVMS/SiNVR Video Server contains a input validation vulnerability, that could allow an unauthenticated remote attacker to cause a Denial-of-Service condition by sending malformed HTTP requests.	7.5	More Details
CVE-2019-3404	By adding some special fields to the uri ofrouter app function, the user could abuse background app cgi functions withoutauthentication. This affects 360 router P0 and F5C.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9544	An issue was discovered on D-Link DSL-2640B E1 EU_1.01 devices. The administrative interface doesn't perform authentication checks for a firmware-update POST request. Any attacker that can access the administrative interface can install firmware of their choice.	7.5	More Details
CVE-2020-6209	SAP Disclosure Management, version 10.1, does not perform necessary authorization checks for an authenticated user, allowing access to administration accounts by a user with no roles, leading to Missing Authorization Check.	7.5	More Details
CVE-2019-17646	An issue was discovered in Centreon before 18.10.8, 19.04.5, and 19.10.2. It provides sensitive information via an unauthenticated direct request for api/external.php?object=centreon_metric&action=listByService.	7.5	More Details
CVE-2019-20502	An issue was discovered in EFS Easy Chat Server 3.1. There is a buffer overflow via a long body2.ghp message parameter.	7.5	More Details
CVE-2020-0034	In vp8_decode_frame of decodeframe.c, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure if error correction were turned on, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1Android ID: A-62458770	7.5	More Details
CVE-2020-6196	SAP BusinessObjects Mobile (MobileBIService), version 4.2, allows an attacker to generate multiple requests, using which he can block all the threads resulting in a Denial of Service.	7.5	More Details
CVE-2020-10184	The verify endpoint in YubiKey Validation Server before 2.40 does not check the length of SQL queries, which allows remote attackers to cause a denial of service, aka SQL injection. NOTE: this issue is potentially relevant to persons outside Yubico who operate a self-hosted OTP validation service; the issue does NOT affect YubiCloud.	7.5	More Details
CVE-2019-19299	A vulnerability has been identified in SiNVR/SiVMS Video Server (All versions < V5.0.0), SiNVR/SiVMS Video Server (All versions >= V5.0.0 < V5.0.2), SiNVR/SiVMS Video Server (All versions >= V5.0.2). The streaming service (default port 5410/tcp) of the SiVMS/SiNVR Video Server applies weak cryptography when exposing device (camera) passwords. This could allow an unauthenticated remote attacker to read and decrypt the passwords and conduct further attacks.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14061	Null-pointer dereference can occur while accessing the segment element info when it is not allocated and assigned in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.5	More Details
CVE-2020-6986	In all versions of Omron PLC CJ Series, an attacker can send a series of specific data packets within a short period, causing a service error on the PLC Ethernet module, which in turn causes a PLC service denied result.	7.5	More Details
CVE-2020-4217	The IBM Spectrum Scale 4.2 and 5.0 file system component is affected by a denial of service security vulnerability. An attacker can force the Spectrum Scale mmfsd/mmsdrserv daemons to unexpectedly exit, impacting the functionality of the Spectrum Scale cluster and the availability of file systems managed by Spectrum Scale. IBM X-Force ID: 175067.	7.5	More Details
CVE-2020-0039	In rw_i93_sm_update_ndef of rw_i93.cc, there is a possible read of uninitialized data due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-143155861	7.5	More Details
CVE-2019-19297	A vulnerability has been identified in SiNVR/SiVMS Video Server (All versions < V5.0.0). The streaming service (default port 5410/tcp) of the SiVMS/SiNVR Video Server contains a path traversal vulnerability, that could allow an unauthenticated remote attacker to access and download arbitrary files from the server.	7.5	More Details
CVE-2019-10549	Null pointer dereference issue can happen due to improper validation of CSEQ header response received from network in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, Nicobar, QCM2150, QM215, Rennell, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDX24, SDX55, SM6150, SM7150, SM8150	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0037	In rw_i93_sm_set_read_only of rw_i93.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-143106535	7.5	More Details
CVE-2020-0038	In rw_i93_sm_update_ndef of rw_i93.cc, there is a possible read of uninitialized data due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-143109193	7.5	More Details
CVE-2019-19223	A Broken Access Control vulnerability in the D-Link DSL-2680 web administration interface (Firmware EU_1.03) allows an attacker to reboot the router by submitting a reboot.html GET request without being authenticated on the admin interface.	7.5	More Details
CVE-2020-10193	ESET Archive Support Module before 1294 allows virus-detection bypass via crafted RAR Compression Information in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.	7.5	More Details
CVE-2019-10591	Null pointer dereference can happen when parsing udta atom which is non-standard and having invalid depth in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8939, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7212	The _encode_invalid_chars function in util/url.py in the urllib3 library 1.25.2 through 1.25.7 for Python allows a denial of service (CPU consumption) because of an inefficient algorithm. The percent_encodings array contains all matches of percent encodings. It is not deduplicated. For a URL of length N, the size of percent_encodings may be up to O(N). The next step (normalize existing percent-encoded bytes) also takes up to O(N) for each step, so the total time is O(N^2). If percent_encodings were deduplicated, the time to compute _encode_invalid_chars would be O(kN), where k is at most 484 ((10+6*2)^2).	7.5	More Details
CVE-2020-10111	Citrix Gateway 11.1, 12.0, and 12.1 has an Inconsistent Interpretation of HTTP Requests. NOTE: Citrix disputes the reported behavior as not a security issue. Citrix ADC only caches HTTP/1.1 traffic for performance optimization	7.5	More Details
CVE-2020-3155	A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.	7.4	More Details
CVE-2020-2146	Jenkins Mac Plugin 1.1.0 and earlier does not validate SSH host keys when connecting agents created by the plugin, enabling man-in-the-middle attacks.	7.4	More Details
CVE-2020-8987	Avast AntiTrack before 1.5.1.172 and AVG Antitrack before 2.0.0.178 proxies traffic to HTTPS sites but does not validate certificates, and thus a man-in-the-middle can host a malicious website using a self-signed certificate. No special action necessary by the victim using AntiTrack with "Allow filtering of HTTPS traffic for tracking detection" enabled. (This is the default configuration.)	7.4	More Details
CVE-2020-0063	In SurfaceFlinger, it is possible to override UI confirmation screen protected by the TEE. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-143128911	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9531	An issue was discovered on Xiaomi MIUI V11.0.5.0.QFAEUXM devices. In the Web resources of GetApps(com.xiaomi.mipicks), the parameters passed in are read and executed. After reading the resource files, relevant components open the link of the incoming URL. Although the URL is safe and can pass security detection, the data carried in the parameters are loaded and executed. An attacker can use NFC tools to get close enough to a user's unlocked phone to cause apps to be installed and information to be leaked. This is fixed on version: 2001122.	7.3	More Details
CVE-2016-11021	setSystemCommand on D-Link DCS-930L devices before 2.12 allows a remote attacker to execute code via an OS command in the SystemCommand parameter.	7.2	More Details
CVE-2015-7342	JNews Joomla Component before 8.5.0 allows SQL injection via upload thumbnail, Queue Search Field, Subscribers Search Field, or Newsletters Search Field.	7.2	More Details
CVE-2015-7338	SQL Injection exists in AcyMailing Joomla Component before 4.9.5 via exportgeolocorder in a geolocation_longitude request to index.php.	7.2	More Details
CVE-2015-7340	JEvents Joomla Component before 3.4.0 RC6 has SQL Injection via evid in a Manage Events action.	7.2	More Details
CVE-2020-6202	SAP NetWeaver Application Server Java (User Management Engine), versions- 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; does not sufficiently validate the LDAP data source configuration XML document accepted from an untrusted source, leading to Missing XML Validation.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3148	A vulnerability in the web-based interface of Cisco Prime Network Registrar (CPNR) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections in the web-based interface. An attacker could exploit this vulnerability by persuading a targeted user, with an active administrative session on the affected device, to click a malicious link. A successful exploit could allow an attacker to change the device's configuration, which could include the ability to edit or create user accounts of any privilege level. Some changes to the device's configuration could negatively impact the availability of networking services for other devices on networks managed by CPNR.	7.1	More Details
CVE-2020-2138	Jenkins Cobertura Plugin 1.15 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	7.1	More Details
CVE-2020-2144	Jenkins Rundeck Plugin 3.6.6 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	7.1	More Details
CVE-2019-14081	Buffer Over-read when WLAN module gets a WMI message for SAR limits with invalid number of limits to be enforced in Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8098, IPQ8074, MSM8998, QCA8081, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM8150, SXR1130	7.1	More Details
CVE-2020-10174	init_tmp in TeeJee.FileSystem.vala in Timeshift before 20.03 unsafely reuses a preexisting temporary directory in the predictable location /tmp/timeshift. It follows symlinks in this location or uses directories owned by unprivileged users. Because Timeshift also executes scripts under this location, an attacker can attempt to win a race condition to replace scripts created by Timeshift with attacker-controlled scripts. Upon success, an attacker-controlled script is executed with full root privileges. This logic is practically always triggered when Timeshift runs regardless of the command-line arguments used.	7.0	More Details
CVE-2020-1706	It has been found that in openshift-enterprise version 3.11 and openshift-enterprise versions 4.1 up to, including 4.3, multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/apb-tools-container.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14072	Unhandled paging request is observed due to dereferencing an already freed object because of race condition between sparse free and sparse bind ioctls which access the same physical entry in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8096AU, APQ8098, MDM9607, MSM8909W, MSM8939, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.0	More Details
CVE-2020-8994	An issue was discovered on XIAOMI AI speaker MDZ-25-DT 1.34.36, and 1.40.14. Attackers can get root shell by accessing the UART interface and then they can read Wi-Fi SSID or password, read the dialogue text files between users and XIAOMI AI speaker, use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, eavesdrop on users and record what XIAOMI AI speaker hears, delete the entire XIAOMI AI speaker system, modify system files, stop voice assistant service, start the XIAOMI AI speaker’s SSH service as a backdoor	6.8	More Details
CVE-2019-19296	A vulnerability has been identified in SiNVR/SiVMS Video Server (All versions < V5.0.0). The two FTP services (default ports 21/tcp and 5411/tcp) of the SiVMS/SiNVR Video Server contain a path traversal vulnerability that could allow an authenticated remote attacker to access and download arbitrary files from the server, if the FTP services are enabled.	6.8	More Details
CVE-2020-0012	In fpc_ta_pn_get_unencrypted_image of fpc_ta_pn.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137648844	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0011	In get_auth_result of fpc_ta_hw_auth.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137648045References: N/A	6.7	More Details
CVE-2020-0010	In fpc_ta_get_build_info of fpc_ta_kpi.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137014293References: N/A	6.7	More Details
CVE-2020-3176	A vulnerability in Cisco Remote PHY Device Software could allow an authenticated, local attacker to execute commands on the underlying Linux shell of an affected device with root privileges. The vulnerability exists because the affected software does not properly sanitize user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability by supplying certain CLI commands with crafted arguments. A successful exploit could allow the attacker to run arbitrary commands as the root user, which could result in a complete system compromise.	6.7	More Details
CVE-2020-0050	In nfa_hciu_send_msg of nfa_hci_utils.cc, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-124521372	6.7	More Details
CVE-2020-0053	In convertHidlNanDataPathInitiatorRequestToLegacy, and convertHidlNanDataPathIndicationResponseToLegacy of hidl_struct_util.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143789898	6.7	More Details
CVE-2016-1159	In ZOHO Password Manager Pro (PMP) 8.3.0 (Build 8303) and 8.4.0 (Build 8400,8401,8402), underprivileged users can obtain sensitive information (entry password history) via a vulnerable hidden service.	6.5	More Details
CVE-2019-19277	A vulnerability has been identified in SIPORT MP (All versions < 3.1.4). Vulnerable versions of the device allow the creation of special accounts ("service users") with administrative privileges that could enable a remote authenticated attacker to perform actions that are not visible to other users of the system, such as granting persons access to a secured area.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-13009	An issue was discovered in GitLab Community and Enterprise Edition 9.2 through 12.0.2. Uploaded files associated with unsaved personal snippets were accessible to unauthorized users due to improper permission settings. It has Incorrect Access Control.	6.5	More Details
CVE-2019-12429	An issue was discovered in GitLab Community and Enterprise Edition 11.9 through 11.11. Unprivileged users were able to access labels, status and merge request counts of confidential issues via the milestone details page. It has Improper Access Control.	6.5	More Details
CVE-2020-0049	In onReadBuffer() of StreamingSource.cpp, there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140177694	6.5	More Details
CVE-2019-19290	A vulnerability has been identified in Control Center Server (CCS) (All versions < V1.5.0). The DOWNLOADS section in the web interface of the Control Center Server (CCS) contains a path traversal vulnerability that could allow an authenticated remote attacker to access and download arbitrary files from the server where CCS is installed.	6.5	More Details
CVE-2020-2139	An arbitrary file write vulnerability in Jenkins Cobertura Plugin 1.15 and earlier allows attackers able to control the coverage report file contents to overwrite any file on the Jenkins master file system.	6.5	More Details
CVE-2019-20503	usrsctp before 2019-12-20 has out-of-bounds reads in sctp_load_addresses_from_init.	6.5	More Details
CVE-2020-10100	An issue was discovered in Zammad 3.0 through 3.2. It allows for users to view ticket customer details associated with specific customers. However, the application does not properly implement access controls related to this functionality. As such, users of one company are able to access ticket data from other companies. Due to the multi-tenant nature of this application, users who can access ticket details from one organization to the next allows for users to exfiltrate potentially sensitive data of other companies.	6.5	More Details
CVE-2020-9530	An issue was discovered on Xiaomi MIUI V11.0.5.0.QFAEUXM devices. The export component of GetApps(com.xiaomi.mipicks) mishandles the functionality of opening other components. Attackers need to induce users to open specific web pages in a specific network environment. By jumping to the WebView component of Messaging(com.android.MMS) and loading malicious web pages, information leakage can occur. This is fixed on version: 2001122; 11.0.1.54.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5405	Spring Cloud Config, versions 2.2.x prior to 2.2.2, versions 2.1.x prior to 2.1.7, and older unsupported versions allow applications to serve arbitrary configuration files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead a directory traversal attack.	6.5	More Details
CVE-2019-14886	A vulnerability was found in business-central, as shipped in rhdm-7.5.1 and rhpam-7.5.1, where encoded passwords are stored in errai_security_context. The encoding used for storing the passwords is Base64, not an encryption algorithm, and any recovery of these passwords could lead to user passwords being exposed.	6.5	More Details
CVE-2020-3181	A vulnerability in the malware detection functionality in Cisco Advanced Malware Protection (AMP) in Cisco AsyncOS Software for Cisco Email Security Appliances (ESAs) could allow an unauthenticated remote attacker to exhaust resources on an affected device. The vulnerability is due to insufficient control over system memory allocation. An attacker could exploit this vulnerability by sending a crafted email through the targeted device. A successful exploit could allow the attacker to cause an email attachment that contains malware to be delivered to a user and cause email processing delays.	6.5	More Details
CVE-2020-8439	Monstra CMS through 3.0.4 allows remote authenticated users to take over arbitrary user accounts via a modified login parameter to an edit URI, as demonstrated by login=victim to the users/21/edit URI.	6.5	More Details
CVE-2020-9282	In Mahara 18.10 before 18.10.5, 19.04 before 19.04.4, and 19.10 before 19.10.2, certain personal information is discoverable inspecting network responses on the 'Edit access' screen when sharing portfolios.	6.5	More Details
CVE-2020-0045	In StatsService::command of StatsService.cpp, there is possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141243101	6.4	More Details
CVE-2020-0066	In the netlink driver, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-65025077	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10706	Western Digital SanDisk SanDisk X300, X300s, X400, and X600 devices: The firmware update authentication method relies on a symmetric HMAC digest. The key used to validate this digest is present in a protected area of the device, and if extracted could be used to install arbitrary firmware to other devices.	6.3	More Details
CVE-2019-19294	A vulnerability has been identified in Control Center Server (CCS) (All versions < V1.5.0). The web interface of the Control Center Server (CCS) contains multiple stored Cross-site Scripting (XSS) vulnerabilities in several input fields. This could allow an authenticated remote attacker to inject malicious JavaScript code into the CCS web application that is later executed in the browser context of any other user who views the relevant CCS web content.	6.3	More Details
CVE-2020-10236	An issue was discovered in Froxlor before 0.10.14. It created files with static names in /tmp during installation if the installation directory was not writable. This allowed local attackers to cause DoS or disclose information out of the config files, because of _createUserdataConf in install/lib/class.FroxlorInstall.php.	6.1	More Details
CVE-2019-11345	Citrix SD-WAN Center 10.2.x before 10.2.1 and NetScaler SD-WAN Center 10.0.x before 10.0.7 allow XSS.	6.1	More Details
CVE-2020-9281	A cross-site scripting (XSS) vulnerability in the HTML Data Processor for CKEditor 4.0 before 4.14 allows remote attackers to inject arbitrary web script through a crafted "protected" comment (with the cke_protected syntax).	6.1	More Details
CVE-2019-12442	An issue was discovered in GitLab Enterprise Edition 11.7 through 11.11. The epic details page contained a lack of input validation and output encoding issue which resulted in a persistent XSS vulnerability on child epics.	6.1	More Details
CVE-2020-10247	MISP 2.4.122 has Persistent XSS in the sighting popover tool. This is related to app/View/Elements/Events/View/sighting_field.ctp.	6.1	More Details
CVE-2019-12444	An issue was discovered in GitLab Community and Enterprise Edition 8.9 through 11.11. Wiki Pages contained a lack of input validation which resulted in a persistent XSS vulnerability.	6.1	More Details
CVE-2020-9440	A cross-site scripting (XSS) vulnerability in the WSC plugin through 5.5.7.5 for CKEditor 4 allows remote attackers to run arbitrary web script inside an IFRAME element by injecting a crafted HTML element into the editor.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6210	SAP Fiori Launchpad, versions- 753, 754, does not sufficiently encode user-controlled inputs, and hence allowing the attacker to inject the meta tag into the launchpad html using the vulnerable parameter, leading to reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2019-19293	A vulnerability has been identified in Control Center Server (CCS) (All versions < V1.5.0). The web interface of the Control Center Server (CCS) contains a reflected Cross-site Scripting (XSS) vulnerability that could allow an unauthenticated remote attacker to steal sensitive data or execute administrative actions on behalf of a legitimate administrator of the CCS web interface.	6.1	More Details
CVE-2020-2140	Jenkins Audit Trail Plugin 3.2 and earlier does not escape the error message for the URL Patterns field form validation, resulting in a reflected cross-site scripting vulnerability.	6.1	More Details
CVE-2020-10246	MISP 2.4.122 has reflected XSS via unsanitized URL parameters. This is related to app/View/Users/statistics_orgs.ctp.	6.1	More Details
CVE-2019-6585	A vulnerability has been identified in SCALANCE S602 (All versions >= V3.0 and < V4.1), SCALANCE S612 (All versions >= V3.0 and < V4.1), SCALANCE S623 (All versions >= V3.0 and < V4.1), SCALANCE S627-2M (All versions >= V3.0 and < V4.1). The integrated configuration web server of the affected devices could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. User interaction is required for a successful exploitation. The user must be logged into the web interface in order for the exploitation to succeed.	6.1	More Details
CVE-2020-7579	A vulnerability has been identified in Spectrum Power™ 5 (All versions < v5.50 HF02). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. User interaction is required for a successful exploitation. If deployed according to recommended system configuration, Siemens consideres the environmental vector as CR:L/IR:M/AR:H/MAV:A (4.1).	6.1	More Details
CVE-2020-3192	A vulnerability in the web-based management interface of Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2152	Jenkins Subversion Release Manager Plugin 1.2 and earlier does not escape the error message for the Repository URL field form validation, resulting in a reflected cross-site scripting vulnerability.	6.1	More Details
CVE-2020-6201	The SAP Commerce (Testweb Extension), versions- 6.6, 6.7, 1808, 1811, 1905, does not sufficiently encode user-controlled inputs, due to which certain GET URL parameters are reflected in the HTTP responses without escaping/sanitization, leading to Reflected Cross Site Scripting.	6.1	More Details
CVE-2020-6205	SAP NetWeaver AS ABAP Business Server Pages (Smart Forms), SAP_BASIS versions- 7.00, 7.01, 7.02, 7.10, 7.11, 7.30, 7.31, 7.40, 7.50, 7.51, 7.52, 7.53, 7.54; does not sufficiently encode user controlled inputs, allowing an unauthenticated attacker to non-permanently deface or modify displayed content and/or steal authentication information of the user and/or impersonate the user and access all information with the same rights as the target user, leading to Reflected Cross Site Scripting Vulnerability.	6.1	More Details
CVE-2020-10192	An issue was discovered in Munkireport before 5.3.0.3923. An unauthenticated actor can send a custom XSS payload through the /report/broken_client endpoint. The payload will be executed by any authenticated users browsing the application. This concerns app/views/listings/default.php.	6.1	More Details
CVE-2019-13010	An issue was discovered in GitLab Enterprise Edition 8.3 through 12.0.2. The color codes decoder was vulnerable to a resource depletion attack if specific formats were used. It allows Uncontrolled Resource Consumption.	5.9	More Details
CVE-2020-3190	A vulnerability in the IPsec packet processor of Cisco IOS XR Software could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition for IPsec sessions to an affected device. The vulnerability is due to improper handling of packets by the IPsec packet processor. An attacker could exploit this vulnerability by sending malicious ICMP error messages to an affected device that get punted to the IPsec packet processor. A successful exploit could allow the attacker to deplete IPsec memory, resulting in all future IPsec packets to an affected device being dropped by the device. Manual intervention is required to recover from this situation.	5.8	More Details
CVE-2019-15034	hw/display/bochs-display.c in QEMU 4.0.0 does not ensure a sufficient PCI config space allocation, leading to a buffer overflow involving the PCIe extended config space.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2145	Jenkins Zephyr Enterprise Test Management Plugin 1.9.1 and earlier stores its Zephyr password in plain text on the Jenkins master file system.	5.5	More Details
CVE-2020-0087	In getProcessPss of ActivityManagerService.java, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127989044	5.5	More Details
CVE-2020-0035	In query of TelephonyProvider.java, there is a possible access to SIM card info due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-140622024	5.5	More Details
CVE-2019-10616	Possibility of null pointer access if the SPDM commands are executed in the non-standard way in TZ. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8016, MDM9150, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8998, SA6155P, SDX24	5.5	More Details
CVE-2020-0059	In btm_ble_batchscan_filter_track_adv_vse_cback of btm_ble_batchscan.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142543524	5.5	More Details
CVE-2020-0061	In Pixel Recorder, there is a possible permissions bypass allowing arbitrary apps to record audio. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-145504977	5.5	More Details
CVE-2020-10237	An issue was discovered in Froxlor through 0.10.15. The installer wrote configuration parameters including passwords into files in /tmp, setting proper permissions only after writing the sensitive data. A local attacker could have disclosed the information if he read the file at the right time, because of _createUserdataConf in install/lib/class.FroxlorInstall.php.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2012-1096	NetworkManager 0.9 and earlier allows local users to use other users' certificates or private keys when making a connection via the file path when adding a new connection.	5.5	More Details
CVE-2020-0048	In onTransact of IAudioFlinger.cpp, there is a possible stack information leak due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139417189	5.5	More Details
CVE-2020-2154	Jenkins Zephyr for JIRA Test Management Plugin 1.5 and earlier stores its credentials in plain text in a global configuration file on the Jenkins master file system.	5.5	More Details
CVE-2020-0055	In l2c_link_process_num_completed_pkts of l2c_link.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141617601	5.5	More Details
CVE-2020-0056	In btu_hcif_connection_comp_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141619686	5.5	More Details
CVE-2020-0057	In btm_process_inq_results of btm_inq.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141620271	5.5	More Details
CVE-2020-4083	HCL Connections 6.5 is vulnerable to possible information leakage. Connections could disclose sensitive information via trace logs to a local user.	5.5	More Details
CVE-2020-10251	In ImageMagick 7.0.9, an out-of-bounds read vulnerability exists within the ReadHEICImageByID function in coders\heic.c. It can be triggered via an image with a width or height value that exceeds the actual size of the image.	5.5	More Details
CVE-2020-10029	The GNU C Library (aka glibc or libc6) before 2.32 could overflow an on-stack buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, a seen when passing a 0x5d414141414141410000 value to sinl on x86 targets. This is related to sysdeps/ieee754/ldbl-96/e_rem_pio2l.c.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11686	Western Digital SanDisk X300, X300s, X400, and X600 devices: A vulnerability in the wear-leveling algorithm of the drive may cause cryptographically sensitive parameters (such as data encryption keys) to remain on the drive media after their intended erasure.	5.5	More Details
CVE-2020-6178	SAP Enable Now, before version 1911, sends the Session ID cookie value in URL. This might be stolen from the browser history or log files, leading to Information Disclosure.	5.4	More Details
CVE-2020-10103	An XSS issue was discovered in Zammad 3.0 through 3.2. Malicious code can be provided by a low-privileged user through the File Upload functionality in Zammad. The malicious JavaScript will execute within the browser of any user who opens a specially crafted link to the uploaded file with an active Zammad session.	5.4	More Details
CVE-2019-4608	IBM Tivoli Workload Scheduler 9.3 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: 168508.	5.4	More Details
CVE-2020-10099	An XSS issue was discovered in Zammad 3.0 through 3.2. Malicious code can be provided by a low-privileged user through the Ticket functionality in Zammad. The malicious JavaScript will execute within the browser of any user who opens the ticket or has the ticket within the Toolbar.	5.4	More Details
CVE-2020-10098	An XSS issue was discovered in Zammad 3.0 through 3.2. Malicious code can be provided by a low-privileged user through the Email functionality. The malicious JavaScript will execute within the browser of any user who opens the Ticket with the Article created from that Email.	5.4	More Details
CVE-2020-10372	Ramp AltitudeCDN Altimeter before 2.4.0 allows authenticated Stored XSS via the vdms/ipmapping.jsp location field to the dms/rest/services/datastore/createOrEditValueForKey URI.	5.4	More Details
CVE-2020-10107	PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to stored XSS, as demonstrated by the ExpenseItem or ExpenseCost parameter in manage-expense.php.	5.4	More Details
CVE-2020-4162	IBM InfoSphere Information Server 11.5 and 11.7 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: 174342.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19773	Various Lexmark products have stored XSS in the embedded web server used in older generation Lexmark devices. Affected products are available in http://support.lexmark.com/index?page=content&id=TE935&locale=en&userlocale=EN_US.	5.4	More Details
CVE-2019-19772	Various Lexmark products have reflected XSS in the embedded web server used in older generation Lexmark devices. Affected products are available in http://support.lexmark.com/index?page=content&id=TE935&locale=en&userlocale=EN_US.	5.4	More Details
CVE-2020-10191	An issue was discovered in MunkiReport before 5.3.0. An authenticated actor can send a custom XSS payload through the /module/comment/save endpoint. The payload will be executed by any authenticated users browsing the application. This concerns app/controllers/client.php:detail.	5.4	More Details
CVE-2020-10112	Citrix Gateway 11.1, 12.0, and 12.1 allows Cache Poisoning. NOTE: Citrix disputes this as not a vulnerability. By default, Citrix ADC only caches static content served under certain URL paths for Citrix Gateway usage. No dynamic content is served under these paths, which implies that those cached pages would not change based on parameter values. All other data traffic going through Citrix Gateway are NOT cached by default	5.4	More Details
CVE-2020-6200	The SAP Commerce (SmartEdit Extension), versions- 6.6, 6.7, 1808, 1811, is vulnerable to client-side angularjs template injection, a variant of Cross-Site-Scripting (XSS) that exploits the templating facilities of the angular framework.	5.4	More Details
CVE-2020-3185	A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data in a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web-based management interface or access sensitive, browser-based information.	5.4	More Details
CVE-2019-12445	An issue was discovered in GitLab Community and Enterprise Edition 8.4 through 11.11. A malicious user could execute JavaScript code on notes by importing a specially crafted project file. It allows XSS.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4084	HCL Connections v5.5, v6.0, and v6.5 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.	5.4	More Details
CVE-2020-6199	The view FIMENAV_COMPCERT in SAP ERP (MENA Certificate Management), EAPPGLO version 607, SAP_FIN versions- 618, 730 and SAP S/4HANA (MENA Certificate Management), S4CORE versions- 100, 101, 102, 103, 104; does not have any authorization check to it due to which an attacker without an authorization group can maintain any company certificate, leading to Missing Authorization Check.	5.4	More Details
CVE-2020-2136	Jenkins Git Plugin 4.2.0 and earlier does not escape the error message for the repository URL for Microsoft TFS field form validation, resulting in a stored cross-site scripting vulnerability.	5.4	More Details
CVE-2020-4082	The HCL Connections 5.5 help system is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.	5.4	More Details
CVE-2020-9517	There is an improper restriction of rendered UI layers or frames vulnerability in Micro Focus Service Manager Release Control versions 9.50 and 9.60. The vulnerability may result in the ability of malicious users to perform UI redress attacks.	5.4	More Details
CVE-2020-3157	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by crafting a malicious configuration and saving it to the targeted system. An exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information when an administrator views the configuration. An attacker would need write permissions to exploit this vulnerability successfully.	5.4	More Details
CVE-2019-19222	A Stored XSS issue in the D-Link DSL-2680 web administration interface (Firmware EU_1.03) allows an authenticated attacker to inject arbitrary JavaScript code into the info.html administration page by sending a crafted Forms/wireless_autonetwork_1 POST request.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19291	A vulnerability has been identified in Control Center Server (CCS) (All versions < V1.5.0), SiNVR/SiVMS Video Server (All versions < V5.0.0). The FTP services of the SiVMS/SiNVR Video Server and the Control Center Server (CCS) maintain log files that store login credentials in cleartext. In configurations where the FTP service is enabled, authenticated remote attackers could extract login credentials of other users of the service.	5.3	More Details
CVE-2020-2143	Jenkins Logstash Plugin 2.3.1 and earlier transmits configured credentials in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.	5.3	More Details
CVE-2020-10110	Citrix Gateway 11.1, 12.0, and 12.1 allows Information Exposure Through Caching. NOTE: Citrix disputes this as not a vulnerability. There is no sensitive information disclosure through the cache headers on Citrix ADC. The "Via" header lists cache protocols and recipients between the start and end points for a request or a response. The "Age" header provides the age of the cached response in seconds. Both headers are commonly used for proxy cache and the information is not sensitive	5.3	More Details
CVE-2020-10249	BWA DiREX-Pro 1.2181 devices allow full path disclosure via an invalid name array parameter to val_soft.php3.	5.3	More Details
CVE-2020-10105	An issue was discovered in Zammad 3.0 through 3.2. It returns source code of static resources when submitting an OPTIONS request, rather than a GET request. Disclosure of source code allows for an attacker to formulate more precise attacks. Source code was disclosed for the file 404.html (/zammad/public/404.html)	5.3	More Details
CVE-2020-10097	An issue was discovered in Zammad 3.0 through 3.2. It may respond with verbose error messages that disclose internal application or infrastructure information. This information could aid attackers in successfully exploiting other vulnerabilities.	5.3	More Details
CVE-2020-10102	An issue was discovered in Zammad 3.0 through 3.2. The Forgot Password functionality is implemented in a way that would enable an anonymous user to guess valid user emails. In the current implementation, the application responds differently depending on whether the input supplied was recognized as associated with a valid user. This behavior could be used as part of a two-stage automated attack. During the first stage, an attacker would iterate through a list of account names to determine which correspond to valid accounts. During the second stage, the attacker would use a list of common passwords to attempt to brute force credentials for accounts that were recognized by the system in the first stage.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9364	An issue was discovered in helpers/mailer.php in the Creative Contact Form extension 4.6.2 before 2019-12-03 for Joomla!. A directory traversal vulnerability resides in the filename field for uploaded attachments via the creativecontactform_upload parameter. An attacker could exploit this vulnerability with the "Send me a copy" option to receive any files of the filesystem via email.	5.3	More Details
CVE-2020-8660	CNCF Envoy through 1.13.0 TLS inspector bypass. TLS inspector could have been bypassed (not recognized as a TLS client) by a client using only TLS 1.3. Because TLS extensions (SNI, ALPN) were not inspected, those connections might have been matched to a wrong filter chain, possibly bypassing some security restrictions in the process.	5.3	More Details
CVE-2020-2155	Jenkins OpenShift Deployer Plugin 1.2.0 and earlier transmits configured credentials in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.	5.3	More Details
CVE-2020-8664	CNCF Envoy through 1.13.0 has incorrect Access Control when using SDS with Combined Validation Context. Using the same secret (e.g. trusted CA) across many resources together with the combined validation context could lead to the “static” part of the validation context to be not applied, even though it was visible in the active config dump.	5.3	More Details
CVE-2020-2149	Jenkins Repository Connector Plugin 1.2.6 and earlier transmits configured credentials in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.	5.3	More Details
CVE-2020-3193	A vulnerability in the web-based management interface of Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to obtain sensitive information about an affected device. The vulnerability exists because replies from the web-based management interface include unnecessary server information. An attacker could exploit this vulnerability by inspecting replies received from the web-based management interface. A successful exploit could allow the attacker to obtain details about the operating system, including the web server version that is running on the device, which could be used to perform further attacks.	5.3	More Details
CVE-2011-4538	Lexmark X, W, T, E, and C devices before 2012-02-09 allow attackers to obtain sensitive information by reading passwords within exported settings.	5.3	More Details
CVE-2020-2151	Jenkins Quality Gates Plugin 2.5 and earlier transmits configured credentials in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2150	Jenkins Sonar Quality Gates Plugin 1.3.1 and earlier transmits configured credentials in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.	5.3	More Details
CVE-2020-3164	A vulnerability in the web-based management interface of Cisco AsyncOS for Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Content Security Management Appliance (SMA) could allow an unauthenticated remote attacker to cause high CPU usage on an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper validation of specific HTTP request headers. An attacker could exploit this vulnerability by sending a malformed HTTP request to an affected device. A successful exploit could allow the attacker to trigger a prolonged status of high CPU utilization relative to the GUI process(es). Upon successful exploitation of this vulnerability, an affected device will still be operative, but its response time and overall performance may be degraded.	5.3	More Details
CVE-2019-12433	An issue was discovered in GitLab Community and Enterprise Edition 11.7 through 11.11. It has Improper Input Validation. Restricted visibility settings allow creating internal projects in private groups, leading to multiple permission issues.	5.3	More Details
CVE-2019-13004	An issue was discovered in GitLab Community and Enterprise Edition 11.10 through 12.0.2. When specific encoded characters were added to comments, the comments section would become inaccessible. It has Incorrect Access Control (issue 1 of 2).	5.3	More Details
CVE-2020-0031	In triggerAugmentedAutofillLocked and related functions of Session.java, it is possible for Augmented Autofill to display sensitive information to the user inappropriately. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141703197	5.0	More Details
CVE-2019-13007	An issue was discovered in GitLab Community and Enterprise Edition 11.11 through 12.0.2. When an admin enabled one of the service templates, it was triggering an action that leads to resource depletion. It allows Uncontrolled Resource Consumption.	4.9	More Details
CVE-2020-9371	Stored XSS exists in the Appointment Booking Calendar plugin before 1.3.35 for WordPress. In the cpabc_appointments.php file, the Calendar Name input could allow attackers to inject arbitrary JavaScript or HTML.	4.8	More Details
CVE-2015-7343	JNews Joomla Component before 8.5.0 has XSS via the mailingsearch parameter.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-7344	HikaShop Joomla Component before 2.6.0 has XSS via an injected payload[/caption].	4.8	More Details
CVE-2020-2137	Jenkins Timestamper Plugin 1.11.1 and earlier does not sanitize HTML formatting of its output, resulting in a stored XSS vulnerability exploitable by attackers with Overall/Administer permission.	4.8	More Details
CVE-2020-0058	In l2c_rcv_acl_data of l2c_main.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141745011	4.4	More Details
CVE-2020-0044	In set_nonce of fpc_ta_qc_auth.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137650219	4.4	More Details
CVE-2020-0043	In authorize_enrol of fpc_ta_hw_auth.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137650218	4.4	More Details
CVE-2020-0042	In fpc_ta_hw_auth_unwrap_key of fpc_ta_hw_auth_qsee.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137649599	4.4	More Details
CVE-2020-0060	In query of SmsProvider.java and MmsSmsProvider.java, there is a possible permission bypass due to SQL injection. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143229845	4.4	More Details
CVE-2019-12431	An issue was discovered in GitLab Community and Enterprise Edition 8.13 through 11.11. Restricted users could access the metadata of private milestones through the Search API. It has Improper Access Control.	4.3	More Details
CVE-2020-2157	Jenkins Skytap Cloud CI Plugin 2.07 and earlier transmits configured credentials in plain text as part of job configuration forms, potentially resulting in their exposure.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10806	vega-util prior to 1.13.1 allows manipulation of object prototype. The 'vega.mergeConfig' method within vega-util could be tricked into adding or modifying properties of the Object.prototype.	4.3	More Details
CVE-2020-2156	Jenkins DeployHub Plugin 8.0.14 and earlier transmits configured credentials in plain text as part of job configuration forms, potentially resulting in their exposure.	4.3	More Details
CVE-2019-12432	An issue was discovered in GitLab Community and Enterprise Edition 8.13 through 11.11. Non-member users who subscribed to issue notifications could access the title of confidential issues through the unsubscription page. It allows Information Disclosure.	4.3	More Details
CVE-2019-13006	An issue was discovered in GitLab Community and Enterprise Edition 9.0 and through 12.0.2. Users with access to issues, but not the repository were able to view the number of related merge requests on an issue. It has Incorrect Access Control.	4.3	More Details
CVE-2020-2141	A cross-site request forgery vulnerability in Jenkins P4 Plugin 1.10.10 and earlier allows attackers to trigger builds or add a labels in Perforce.	4.3	More Details
CVE-2019-12434	An issue was discovered in GitLab Community and Enterprise Edition 10.6 through 11.11. Users could guess the URL slug of private projects through the contrast of the destination URLs of issues linked in comments. It allows Information Disclosure.	4.3	More Details
CVE-2019-13005	An issue was discovered in GitLab Enterprise Edition and Community Edition 1.10 through 12.0.2. The GitLab graphql service was vulnerable to multiple authorization issues that disclosed restricted user, group, and repository metadata to unauthorized users. It has Incorrect Access Control.	4.3	More Details
CVE-2020-3182	A vulnerability in the multicast DNS (mDNS) protocol configuration of Cisco Webex Meetings Client for MacOS could allow an unauthenticated adjacent attacker to obtain sensitive information about the device on which the Webex client is running. The vulnerability exists because sensitive information is included in the mDNS reply. An attacker could exploit this vulnerability by doing an mDNS query for a particular service against an affected device. A successful exploit could allow the attacker to gain access to sensitive information.	4.3	More Details
CVE-2019-13002	An issue was discovered in GitLab Community and Enterprise Edition 11.10 through 12.0.2. Unauthorized users were able to read pipeline information of the last merge request. It has Incorrect Access Control.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0052	In smsSelected of AnswerFragment.java, there is a way to send an SMS from the lock screen due to a permissions bypass. This could lead to local escalation of privilege on the lock screen with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-137102479	4.3	More Details
CVE-2019-13011	An issue was discovered in GitLab Enterprise Edition 8.11.0 through 12.0.2. By using brute-force a user with access to a project, but not it's repository could create a list of merge requests template names. It has excessive algorithmic complexity.	4.3	More Details
CVE-2020-9386	In Mahara 18.10 before 18.10.5, 19.04 before 19.04.4, and 19.10 before 19.10.2, file metadata information is disclosed to group members in the Elasticsearch result list despite them not having access to that artefact anymore.	4.3	More Details
CVE-2015-7968	nwbc_ext2int in SAP NetWeaver Application Server before Security Note 2183189 allows XXE attacks for local file inclusion via the sap/bc/ui2/nwbc/nwbc_ext2int/ URI.	4.3	More Details
CVE-2019-13001	An issue was discovered in GitLab Community and Enterprise Edition 11.9 and later through 12.0.2. GitLab Snippets were vulnerable to an authorization issue that allowed unauthorized users to add comments to a private snippet. It allows authentication bypass.	4.3	More Details
CVE-2020-2142	A missing permission check in Jenkins P4 Plugin 1.10.10 and earlier allows attackers with Overall/Read permission to trigger builds.	4.3	More Details
CVE-2020-9455	The RegistrationMagic plugin through 4.6.0.3 for WordPress allows remote authenticated users (with minimal privileges) to send arbitrary emails on behalf of the site via class_rm_user_services.php send_email_user_view.	4.3	More Details
CVE-2019-19295	A vulnerability has been identified in Control Center Server (CCS) (All versions < V1.5.0). The Control Center Server (CCS) does not enforce logging of security-relevant activities in its XML-based communication protocol as provided by default on ports 5444/tcp and 5440/tcp. An authenticated remote attacker could exploit this vulnerability to perform covert actions that are not visible in the application log.	4.3	More Details
CVE-2020-6206	SAP Cloud Platform Integration for Data Services, version 1.0, allows user inputs to be reflected as error or warning massages. This could mislead the victim to follow malicious instructions inserted by external attackers, leading to Cross Site Request Forgery.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2148	A missing permission check in Jenkins Mac Plugin 1.1.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified SSH server using attacker-specified credentials.	4.3	More Details
CVE-2020-6204	The selection query in SAP Treasury and Risk Management (Transaction Management) (EA-FINSERV?versions 600, 603, 604, 605, 606, 616, 617, 618, 800 and S4CORE versions 101, 102, 103, 104) returns more records than it should be when selecting and displaying the contract number, leading to Missing Authorization Check.	4.3	More Details
CVE-2020-2153	Jenkins Backlog Plugin 2.4 and earlier transmits configured credentials in plain text as part of job configuration forms, potentially resulting in their exposure.	4.3	More Details
CVE-2019-10065	An issue was discovered in Open Ticket Request System (OTRS) 7.0 through 7.0.6. An attacker who is logged into OTRS as a customer user can use the search result screens to disclose information from internal FAQ articles, a different vulnerability than CVE-2019-9753.	4.3	More Details
CVE-2020-10104	An issue was discovered in Zammad 3.0 through 3.2. After authentication, it transmits sensitive information to the user that may be compromised and used by an attacker to gain unauthorized access. Hashed passwords are returned to the user when visiting a certain URL.	4.3	More Details
CVE-2020-2147	A cross-site request forgery vulnerability in Jenkins Mac Plugin 1.1.0 and earlier allows attackers to connect to an attacker-specified SSH server using attacker-specified credentials.	4.3	More Details
CVE-2019-13457	An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.8. A customer user can use the search results to disclose information from their "company" tickets (with the same CustomerID), even when the CustomerDisableCompanyTicketAccess setting is turned on.	4.3	More Details
CVE-2020-5253	NetHack before version 3.6.0 allowed malicious use of escaping of characters in the configuration file (usually .nethackrc) which could be exploited. This bug is patched in NetHack 3.6.0.	3.9	More Details
CVE-2020-5254	In NetHack before 3.6.6, some out-of-bound values for the hilite_status option can be exploited. NetHack 3.6.6 resolves this issue.	3.9	More Details
CVE-2019-20382	QEMU 4.1.0 has a memory leak in zrle_compress_data in ui/vnc-enc-zrle.c during a VNC disconnect operation because libz is misused, resulting in a situation where memory allocated in deflateInit2 is not freed in deflateEnd.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6197	SAP Enable Now, before version 1908, does not invalidate session tokens in a timely manner. The Insufficient Session Expiration may allow attackers with local access, for instance, to still download the portables.	3.3	More Details
CVE-2020-0047	In setMasterMute of AudioService.java, there is a missing permission check. This could lead to local silencing of audio with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141622311	3.3	More Details
CVE-2020-0029	In the WifiConfigManager, there is a possible storage of location history which can only be deleted by triggering a factory reset. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140065828	2.3	More Details
CVE-2019-14503	Rejected reason: Unused CVE for 2019	N/A	More Details
CVE-2017-14208	Rejected reason: Unused CVE for 2017	N/A	More Details
CVE-2019-8401	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2017-14203	Rejected reason: Unused CVE for 2017	N/A	More Details
CVE-2017-14204	Rejected reason: Unused CVE for 2017	N/A	More Details
CVE-2017-14205	Rejected reason: Unused CVE for 2017	N/A	More Details
CVE-2017-14206	Rejected reason: Unused CVE for 2017	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10020	Rejected reason: Number assigned to issue that does not qualify for a CVE	N/A	More Details
CVE-2017-14207	Rejected reason: Unused CVE for 2017	N/A	More Details
CVE-2019-14508	Rejected reason: Unused CVE for 2019	N/A	More Details
CVE-2019-14499	Rejected reason: Unused CVE for 2019	N/A	More Details
CVE-2019-20226	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-14507	Rejected reason: Unused CVE for 2019	N/A	More Details
CVE-2019-14506	Rejected reason: Unused CVE for 2019	N/A	More Details
CVE-2020-10175	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-2019-14500	Rejected reason: Unused CVE for 2019	N/A	More Details
CVE-2019-14501	Rejected reason: Unused CVE for 2019	N/A	More Details
CVE-2019-20509	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it only affected a development version. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14505	Rejected reason: Unused CVE for 2019	N/A	More Details
CVE-2019-14502	Rejected reason: Unused CVE for 2019	N/A	More Details
CVE-2019-14504	Rejected reason: Unused CVE for 2019	N/A	More Details
CVE-2020-7975	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details