SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 17 June 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-2019-4576	IBM QRadar Network Packet Capture 7.3.0 - 7.3.3 Patch 1 and 7.4.0 GA does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 166803.	9.8	More Details
CVE-2020-0595	Use after free in IPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	9.8	More Details
CVE-2020-4469	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. This vulnerability is due to an incomplete fix for CVE-2020-4211. IBM X-Force ID: 181724.	9.8	More Details
CVE-2020-14011	Lansweeper 6.0.x through 7.2.x has a default installation in which the admin password is configured for the admin account, unless "Built-in admin" is manually unchecked. This allows command execution via the Add New Package and Scheduled Deployments features.	9.8	More Details
CVE-2020-14054	SOKKIA GNR5 Vanguard WEB version 1.2 (build: 91f2b2c3a04d203d79862f87e2440cb7cefc3cd3) and hardware version 212 allows remote attackers to bypass admin authentication via a SQL injection attack that uses the User Name or Password field on the login page.	9.8	More Details
CVE-2018-21246	Caddy before 0.10.13 mishandles TLS client authentication, as demonstrated by an authentication bypass caused by the lack of the StrictHostMatching mode.	9.8	More Details
CVE-2020-14033	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_streaming_rtsp_parse_sdp in plugins/janus_streaming.c has a Buffer Overflow via a crafted RTSP server.	9.8	More Details
CVE-2020-14034	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_get_codec_from_pt in utils.c has a Buffer Overflow via long value in an SDP Offer packet.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11969	If Apache TomEE is configured to use the embedded ActiveMQ broker, and the broker URI includes the useJMX=true parameter, a JMX port is opened on TCP port 1099, which does not include authentication. This affects Apache TomEE 8.0.0-M1 - 8.0.1, Apache TomEE 7.1.0 - 7.1.2, Apache TomEE 7.0.0-M1 - 7.0.7, Apache TomEE 1.0.0 - 1.7.5.	9.8	More Details
CVE-2020-12001	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. The parsing mechanism that processes certain file types does not provide input sanitation. This may allow an attacker to use specially crafted files to traverse the file system and modify or expose sensitive data or execute arbitrary code.	9.8	More Details
CVE-2020-12019	WebAccess Node Version 8.4.4 and prior is vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute arbitrary code.	9.8	More Details
CVE-2020-0223	This is an unbounded write into kernel global memory, via a user-controlled buffer size.Product: AndroidVersions: Android kernelAndroid ID: A-135130450	9.8	More Details
CVE-2020-0232	Function abc_pcie_issue_dma_xfer_sync creates a transfer object, adds it to the session object then continues to work with it. A concurrent thread could retrieve created transfer object from the session object and delete it using abc_pcie_dma_user_xfer_clean. If this happens, abc_pcie_start_dma_xfer and abc_pcie_wait_dma_xfer in the original thread will trigger UAF when working with the transfer object.Product: AndroidVersions: Android kernelAndroid ID: A-151453714	9.8	More Details
CVE-2020-0235	In crus_sp_shared_ioctl we first copy 4 bytes from userdata into "size" variable, and then use that variable as the size parameter for "copy_from_user", ending up overwriting memory following "crus_sp_hdr". "crus_sp_hdr" is a static variable, of type "struct crus_sp_ioctl_header".Product: AndroidVersions: Android kernelAndroid ID: A-135129430	9.8	More Details
CVE-2020-9296	Netflix Titus uses Java Bean Validation (JSR 380) custom constraint validators. When building custom constraint violation error messages, different types of interpolation are supported, including Java EL expressions. If an attacker can inject arbitrary data in the error message template being passed to ConstraintValidatorContext.buildConstraintViolationWithTemplate() argument, they will be able to run arbitrary Java code.	9.8	More Details
CVE-2020-7497	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD)which could cause arbitrary application execution when the computer starts.	9.8	More Details
CVE-2020-7498	A CWE-798: Use of Hard-coded Credentials vulnerability exists in the Unity Loader and OS Loader Software (all versions). The fixed credentials are used to simplify file transfer. Today the use of fixed credentials is considered a vulnerability, which could cause unauthorized access to the file transfer service provided by the Modicon PLCs. This could result in various unintended results.	9.8	More Details
CVE-2020-7500	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered.	9.8	More Details
CVE-2020-7508	A CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to gain full access by brute force.	9.8	More Details
CVE-2020-6263	Standalone clients connecting to SAP NetWeaver AS Java via P4 Protocol, versions (SAP-JEECOR 7.00, 7.01; SERVERCOR 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; CORE-TOOLS 7.00, 7.01, 7.02, 7.05, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50) do not perform any authentication checks for operations that require user identity leading to Authentication Bypass.	9.8	More Details
CVE-2020-4216	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 175066.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0594	Out-of-bounds read in IPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	9.8	More Details
CVE-2020-14080	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an unauthenticated user to execute arbitrary code by POSTing to apply_sec.cgi via the action ping_test with a sufficiently long ping_ipaddr key.	9.8	More Details
CVE-2020-6275	SAP Netweaver AS ABAP, versions 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, are vulnerable for Server Side Request Forgery Attack where in an attacker can use inappropriate path names containing malicious server names in the import/export of sessions functionality and coerce the web server into authenticating with the malicious server. Furthermore, if NTLM is setup the attacker can compromise confidentiality, integrity and availability of the SAP database.	9.8	More Details
CVE-2020-7673	node-extend through 0.2.0 is vulnerable to Arbitrary Code Execution. User input provided to the argument `A` of `extend` function`(A,B,as,isAargs)` located within `lib/extend.js` is executed by the `eval` function, resulting in code execution.	9.8	More Details
CVE-2020-7674	access-policy through 3.1.0 is vulnerable to Arbitrary Code Execution. User input provided to the `template` function is executed by the `eval` function resulting in code execution.	9.8	More Details
CVE-2020-7675	cd-messenger through 2.7.26 is vulnerable to Arbitrary Code Execution. User input provided to the `color` argument executed by the `eval` function resulting in code execution.	9.8	More Details
CVE-2020-0117	In aes_cmac of aes_cmac.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution in the bluetooth server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-151155194	9.8	More Details
CVE-2020-12757	HashiCorp Vault and Vault Enterprise 1.4.0 and 1.4.1, when configured with the GCP Secrets Engine, may incorrectly generate GCP Credentials with the default time-to-live lease duration instead of the engine-configured setting. This may lead to generated GCP credentials being valid for longer than intended. Fixed in 1.4.2.	9.8	More Details
CVE-2020-13901	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_sdp_merge in sdp.c has a stack-based buffer overflow.	9.8	More Details
CVE-2020-13854	Artica Pandora FMS 7.44 allows privilege escalation.	9.8	More Details
CVE-2020-4101	"HCL Digital Experience is susceptible to Server Side Request Forgery."	9.8	More Details
CVE-2020-0138	In get_element_attr_rsp of btif_rc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution if bluetoothtbd were used, which it isn't in typical Android platforms, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142878416	9.8	More Details
CVE-2020-0201	In showSecurityFields of WifiConfigController.java there is a possible credential leak due to a confused deputy. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143601727	9.8	More Details
CVE-2020-0217	In RW_T4tPresenceCheck of rw_t4t.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141331405	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9633	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-13656	In Morgan Stanley Hobbes through 2020-05-21, the array implementation lacks bounds checking, allowing exploitation of an out-of-bounds (OOB) read/write vulnerability that leads to both local and remote code (via RPC) execution.	9.8	More Details
CVE-2020-14067	The install_from_hash functionality in Navigate CMS 2.9 does not consider the .phtml extension when examining files within a ZIP archive that may contain PHP code, in check_upload in lib/packages/extensions/extension.class.php and lib/packages/themes/theme.class.php.	9.8	More Details
CVE-2020-7512	A CWE-1103: Use of Platform-Dependent Third Party Components with vulnerabilities vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to exploit the component.	9.8	More Details
CVE-2020-5754	Webroot endpoint agents prior to version v9.0.28.48 allows remote attackers to trigger a type confusion vulnerability over its listening TCP port, resulting in crashing or reading memory contents of the Webroot endpoint agent.	9.1	More Details
CVE-2020-7589	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). The vulnerability could lead to an attacker reading and modifying the device configuration and obtain project files from affected devices. The security vulnerability could be exploited by an unauthenticated attacker with network access to port 135/tcp. No user interaction is required to exploit this security vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.	9.1	More Details
CVE-2018-21245	Pound before 2.8 allows HTTP request smuggling, a related issue to CVE-2016-10711.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-9635	Adobe Framemaker versions 2019.0.5 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-7503	A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to execute malicious commands on behalf of a legitimate user when xsrf-token data is intercepted.	8.8	More Details
CVE-2020-7501	A CWE-798: Use of Hard-coded Credentials vulnerability exists in Vijeo Designer Basic (V1.1 HotFix 16 and prior) and Vijeo Designer (V6.2 SP9 and prior) which could cause unauthorized read and write when downloading and uploading project or firmware into Vijeo Designer Basic and Vijeo Designer.	8.8	More Details
CVE-2020-14075	TRENDnet TEW-827DRU devices through 2.06B04 contain multiple command injections in apply.cgi via the action pppoe_connect, ru_pppoe_connect, or dhcp_connect with the key wan_ifname (or wan0_dns), allowing an authenticated user to run arbitrary commands on the device.	8.8	More Details
CVE-2020-14077	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action set_sta_enrollee_pin_wifi1 (or set_sta_enrollee_pin_wifi0) with a sufficiently long wps_sta_enrollee_pin key.	8.8	More Details
CVE-2020-14078	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action wifi_captive_portal_login with a sufficiently long REMOTE_ADDR key.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0194	In ihevcd_parse_slice_header of ihevcd_parse_slice_header.c, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143826590	8.8	More Details
CVE-2020-14079	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action auto_up_fw (or auto_up_lp) with a sufficiently long update_file_name key.	8.8	More Details
CVE-2020-14081	TRENDnet TEW-827DRU devices through 2.06B04 contain multiple command injections in apply.cgi via the action send_log_email with the key auth_acname (or auth_passwd), allowing an authenticated user to run arbitrary commands on the device.	8.8	More Details
CVE-2020-14076	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action st_dev_connect, st_dev_disconnect, or st_dev_rconnect with a sufficiently long wan_type key.	8.8	More Details
CVE-2019-19109	The wpForo plugin 1.6.5 for WordPress allows wp-admin/admin.php?page=wpforo-usergroups CSRF.	8.8	More Details
CVE-2020-0168	In impeg2_fmt_conv_yuv420p_to_yuv420sp_uv of impeg2_format_conv.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-137798382	8.8	More Details
CVE-2020-0160	In setSyncSampleParams of SampleTable.cpp, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-124771364	8.8	More Details
CVE-2020-14156	user_channel/passwd_mgr.cpp in OpenBMC phosphor-host-ipmid before 2020-04-03 does not ensure that /etc/ipmi-pass has strong file permissions.	8.8	More Details
CVE-2020-9634	Adobe Framemaker versions 2019.0.5 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-14159	By using an Automate API in ConnectWise Automate before 2020.5.178, a remote authenticated user could execute commands and/or modifications within an individual Automate instance by triggering an SQL injection vulnerability in /LabTech/agent.aspx. This affects versions before 2019.12.337, 2020 before 2020.1.53, 2020.2 before 2020.2.85, 2020.3 before 2020.3.114, 2020.4 before 2020.4.143, and 2020.5 before 2020.5.178.	8.8	More Details
CVE-2020-13445	In Liferay Portal before 7.3.2 and Liferay DXP 7.0 before fix pack 92, 7.1 before fix pack 18, and 7.2 before fix pack 6, the template API does not restrict user access to sensitive objects, which allows remote authenticated users to execute arbitrary code via crafted FreeMarker and Velocity templates.	8.8	More Details
CVE-2020-13905	IrfanView 4.54 allows a user-mode write access violation starting at FORMATS!GetPlugInInfo+0x0000000000038ed4.	8.8	More Details
CVE-2020-0131	In parseChunk of MPEG4Extractor.cpp, there is a possible out of bounds write due to incompletely initialized data. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-151159638	8.8	More Details
CVE-2020-5742	Improper Access Control in Plex Media Server prior to June 15, 2020 allows any origin to execute cross-origin application requests.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5593	Zenphoto versions prior to 1.5.7 allows an attacker to conduct PHP code injection attacks by leading a user to upload a specially crafted .zip file.	8.8	More Details
CVE-2020-14074	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action kick_ban_wifi_mac_allow with a sufficiently long qcawifi.wifi0_vap0.maclist key.	8.8	More Details
CVE-2020-0190	In ideint_weave_blk of ideint_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-10Android ID: A-140324890	8.8	More Details
CVE-2020-13851	Artica Pandora FMS 7.44 allows remote command execution via the events feature.	8.8	More Details
CVE-2020-9636	Adobe Framemaker versions 2019.0.5 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-14212	FFmpeg through 4.3 has a heap-based buffer overflow in avio_get_str in libavformat/aviobuf.c because dnn_backend_native.c calls ff_dnn_load_model_native and a certain index check is omitted.	8.8	More Details
CVE-2020-5363	Select Dell Client Consumer and Commercial platforms include an issue that allows the BIOS Admin password to be changed through Dell's manageability interface without knowledge of the current BIOS Admin password. This could potentially allow an unauthorized actor, with physical access and/or OS administrator privileges to the device, to gain privileged access to the platform and the hard drive.	8.6	More Details
CVE-2020-7672	mosc through 1.0.0 is vulnerable to Arbitrary Code Execution. User input provided to `properties` argument is executed by the `eval` function, resulting in code execution.	8.6	More Details
CVE-2020-6271	SAP Solution Manager (Problem Context Manager), version 7.2, does not perform the necessary authentication, allowing an attacker to consume large amounts of memory, causing the system to crash and read restricted data (files visible for technical administration users of the diagnostics agent).	8.2	More Details
CVE-2020-14195	FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to org.jsecurity.realm.jndi.JndiRealmFactory (aka org.jsecurity).	8.1	More Details
CVE-2020-5411	When configured to enable default typing, Jackson contained a deserialization vulnerability that could lead to arbitrary code execution. Jackson fixed this vulnerability by blacklisting known "deserialization gadgets". Spring Batch configures Jackson with global default typing enabled which means that through the previous exploit, arbitrary code could be executed if all of the following is true: * Spring Batch's Jackson support is being leveraged to serialize a job's ExecutionContext. * A malicious user gains write access to the data store used by the JobRepository (where the data to be deserialized is stored). In order to protect against this type of attack, Jackson prevents a set of untrusted gadget classes from being deserialized. Spring Batch should be proactive against blocking unknown "deserialization gadgets" when enabling default typing.	8.1	More Details
CVE-2020-11999	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. An exposed API call allows users to provide files to be processed without sanitation. This may allow an attacker to specify a filename to execute unauthorized code and modify files or data.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11614	Mids' Reborn Hero Designer 2.6.0.7 downloads the update manifest, as well as update files, over cleartext HTTP. Additionally, the application does not perform file integrity validation for files after download. An attacker can perform a man-in-the-middle attack against this connection and replace executable files with malicious versions, which the operating system then executes under the context of the user running Hero Designer.	8.1	More Details
CVE-2020-14060	FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to oadd.org.apache.xalan.lib.sql.JNDIConnectionPool (aka apache/drill).	8.1	More Details
CVE-2020-14062	FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to com.sun.org.apache.xalan.internal.lib.sql.JNDIConnectionPool (aka xalan2).	8.1	More Details
CVE-2020-6268	Statutory Reporting for Insurance Companies in SAP ERP (EA-FINSERV versions - 600, 603, 604, 605, 606, 616, 617, 618, 800 and S4CORE versions 101, 102, 103, 104) does not execute the required authorization checks for an authenticated user, allowing an attacker to view and tamper with certain restricted data leading to Missing Authorization Check.	8.1	More Details
CVE-2020-14061	FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to oracle.jms.AQjmsQueueConnectionFactory, oracle.jms.AQjmsXATopicConnectionFactory, oracle.jms.AQjmsTopicConnectionFactory, oracle.jms.AQjmsXAQueueConnectionFactory, and oracle.jms.AQjmsXAConnectionFactory (aka weblogic/oracle-aqjms).	8.1	More Details
CVE-2020-4470	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 Administrative Console could allow an authenticated attacker to upload arbitrary files which could be execute arbitrary code on the vulnerable server. IBM X-Force ID: 181725.	8.0	More Details
CVE-2020-0210	In removeSharedAccountAsUser of AccountManager.java, there is a possible permissions bypass to a confused deputy. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145206763	7.8	More Details
CVE-2020-0216	In phNciNfc_RecvMfResp of phNxpExtns_MifareStd.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-126204073	7.8	More Details
CVE-2020-0203	In freeIsolatedUidLocked of ProcessList.java, there is a possible UID reuse due to improper cleanup. This could lead to local escalation of privilege between constrained processes with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146313311	7.8	More Details
CVE-2020-5755	Webroot endpoint agents prior to version v9.0.28.48 did not protect the "%PROGRAMDATA%\WrData\PKG" directory against renaming. This could allow attackers to trigger a crash or wait upon Webroot service restart to rewrite and hijack dlls in this directory for privilege escalation.	7.8	More Details
CVE-2020-0129	In SetData of btm_ble_multi_adv.cc, there is a possible out-of-bound 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-10Android ID: A-123292010	7.8	More Details
CVE-2020-0208	In multiple functions of AccountManager.java, there is a possible 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-10Android ID: A-145207098	7.8	More Details
CVE-2020-0209	In multiple functions of AccountManager.java, there is a possible 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-10Android ID: A-145206842	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11613	Mids' Reborn Hero Designer 2.6.0.7 has an elevation of privilege vulnerability due to default and insecure permissions being set for the installation folder. By default, the Authenticated Users group has Modify permissions to the installation folder. Because of this, any user on the system can replace binaries or plant malicious DLLs to obtain elevated, or different, privileges, depending on the context of the user that runs the application.	7.8	More Details
CVE-2020-0233	In main of main.cpp, there is possible memory corruption due to a use after free. 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-150225255	7.8	More Details
CVE-2020-13651	An issue was discovered in DigDash 2018R2 before p20200528, 2019R1 before p20200421, and 2019R2 before p20200430. It allows a user to provide data that will be used to generate the JNLP file used by a client to obtain the right Java application. By providing an attacker-controlled URL, the client will obtain a rogue JNLP file specifying the installation of malicious JAR archives and executed with full privileges on the client computer.	7.8	More Details
CVE-2020-0136	In multiple locations of Parcel.cpp, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege in the system server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-120078455	7.8	More Details
CVE-2020-0219	In onCreate of SliceDeepLinkSpringBoard.java there is a possible insecure Intent. This could lead to local elevation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-122836081	7.8	More Details
CVE-2020-0150	In rw_t3t_message_set_block_list of rw_t3t.cc, there is a possible out of bounds write due to a missing 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-10Android ID: A-142280329	7.8	More Details
CVE-2020-0188	In onCreatePermissionRequest of SettingsSliceProvider.java, there is a possible permissions bypass due to a PendingIntent error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-147355897	7.8	More Details
CVE-2020-3961	VMware Horizon Client for Windows (prior to 5.4.3) contains a privilege escalation vulnerability due to folder permission configuration and unsafe loading of libraries. A local user on the system where the software is installed may exploit this issue to run commands as any user.	7.8	More Details
CVE-2020-13150	D-link DSL-2750U ISL2750UEME3.V1E devices allow approximately 90 seconds of access to the control panel, after a restart, before MAC address filtering rules become active.	7.8	More Details
CVE-2020-0155	In phNxpNciHal_send_ese_hal_cmd of phNxpNciHal_ext.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139736386	7.8	More Details
CVE-2020-0215	In onCreate of ConfirmConnectActivity.java, there is a possible leak of Bluetooth information due to a permissions bypass. This could lead to local escalation of privilege that exposes a pairing Bluetooth MAC address with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-9 Android-10 Android-11 Android-8.0 Android-8.1 Android ID: A-140417248	7.8	More Details
CVE-2020-0202	In onHandleIntent of TraceService.java, there is a possible bypass of developer settings requirements for capturing system traces due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-11 Android ID: A-142936525	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14004	An issue was discovered in Icinga2 before v2.12.0-rc1. The prepare-dirs script (run as part of the icinga2 systemd service) executes chmod 2750 /run/icinga2/cmd. /run/icinga2 is under control of an unprivileged user by default. If /run/icinga2/cmd is a symlink, then it will by followed and arbitrary files can be changed to mode 2750 by the unprivileged icinga2 user.	7.8	More Details
CVE-2020-13431	I2P before 0.9.46 allows local users to gain privileges via a Trojan horse I2PSvc.exe file because of weak permissions on a certain %PROGRAMFILES% subdirectory.	7.8	More Details
CVE-2020-0586	Improper initialization in subsystem for Intel(R) SPS versions before SPS_E3_04.01.04.109.0 and SPS_E3_04.08.04.070.0 may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access.	7.8	More Details
CVE-2020-0542	Improper buffer restrictions in subsystem for Intel(R) CSME versions before 12.0.64, 13.0.32, 14.0.33 and 14.5.12 may allow an authenticated user to potentially enable escalation of privilege, information disclosure or denial of service via local access.	7.8	More Details
CVE-2020-0179	In doSendObjectInfo of MtpServer.cpp, there is a possible path traversal attack due to insufficient input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is required for exploitation.Product: AndroidVersions: Android-10Android ID: A-130656917	7.8	More Details
CVE-2020-0183	In handleMessage of BluetoothManagerService, there is an incomplete reset. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-110181479	7.8	More Details
CVE-2020-0529	Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-0528	Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access.	7.8	More Details
CVE-2020-0166	In multiple functions of URI.java, there is a possible escalation of privilege due to missing validation in the parceling of URI information. This could lead to a local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-124526860	7.8	More Details
CVE-2020-0137	In setIPv6AddrGenMode of NetworkManagementService.java, there is a possible bypass of networking permissions 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-141920289	7.8	More Details
CVE-2020-0234	In crus_afe_get_param of msm-cirrus-playback.c, there is a possible out of bounds write due to a missing 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-148189280	7.8	More Details
CVE-2020-7496	A CWE-88: Argument Injection or Modification vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD)which could cause unauthorized write access when opening the project file.	7.8	More Details
CVE-2020-7493	A CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD) which could cause malicious code execution when opening the project file.	7.8	More Details
CVE-2020-0114	In onCreateSliceProvider of KeyguardSliceProvider.java, there is a possible confused deputy due to a PendingIntent error. This could lead to local escalation of privilege that allows actions performed as the System UI, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-147606347	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7585	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions < V9.2), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF2). A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information.	7.8	More Details
CVE-2020-2026	A malicious guest compromised before a container creation (e.g. a malicious guest image or a guest running multiple containers) can trick the kata runtime into mounting the untrusted container filesystem on any host path, potentially allowing for code execution on the host. This issue affects: Kata Containers 1.11 versions earlier than 1.11.1; Kata Containers 1.10 versions earlier than 1.10.5; Kata Containers 1.9 and earlier versions.	7.8	More Details
CVE-2020-0115	In verifyIntentFiltersIfNeeded of PackageManagerService.java, there is a possible settings bypass allowing an app to become the default handler for arbitrary domains. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-150038428	7.8	More Details
CVE-2020-7586	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions < V9.2), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF2). A buffer overflow vulnerability could allow a local attacker to cause a Denial-of-Service situation. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information.	7.8	More Details
CVE-2020-7280	Privilege Escalation vulnerability during daily DAT updates when using McAfee Virus Scan Enterprise (VSE) prior to 8.8 Patch 15 allows local users to cause the deletion and creation of files they would not normally have permission to through altering the target of symbolic links. This is timing dependent.	7.8	More Details
CVE-2020-13906	IrfanView 4.54 allows a user-mode write access violation starting at FORMATS!GetPlugInInfo+0x0000000000038eb7.	7.8	More Details
CVE-2019-18614	On the Cypress CYW20735 evaluation board, any data that exceeds 384 bytes is copied and causes an overflow. This is because the maximum BLOC buffer size for sending and receiving data is set to 384 bytes, but everything else is still configured to the usual size of 1092 (which was used for everything in the previous CYW20719 and later CYW20819 evaluation board). To trigger the overflow, an attacker can either send packets over the air or as unprivileged local user. Over the air, the minimal PoC is sending "l2ping -s 600" to the target address prior to any pairing. Locally, the buffer overflow is immediately triggered by opening an ACL or SCO connection to a headset. This occurs because, in WICED Studio 6.2 and 6.4, BT_ACL_HOST_TO_DEVICE_DEFAULT_SIZE and BT_ACL_DEVICE_TO_HOST_DEFAULT_SIZE are set to 384.	7.8	More Details
CVE-2020-0118	In addListener of RegionSamplingThread.cpp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-150904694	7.8	More Details
CVE-2020-7494	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD) which could cause malicious code execution when opening the project file.	7.8	More Details
CVE-2020-14147	An integer overflow in the getnum function in lua_struct.c in Redis before 6.0.3 allows context-dependent attackers with permission to run Lua code in a Redis session to cause a denial of service (memory corruption and application crash) or possibly bypass intended sandbox restrictions via a large number, which triggers a stack-based buffer overflow. NOTE: this issue exists because of a CVE-2015-8080 regression.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4043	phpMussel from versions 1.0.0 and less than 1.6.0 has an unserialization vulnerability in PHP's phar wrapper. Uploading a specially crafted file to an affected version allows arbitrary code execution (discovered, tested, and confirmed by myself), so the risk factor should be regarded as very high. Newer phpMussel versions don't use PHP's phar wrapper, and are therefore unaffected. This has been fixed in version 1.6.0.	7.7	More Details
CVE-2020-7671	goliath through 1.0.6 allows request smuggling attacks where goliath is used as a backend and a frontend proxy also being vulnerable. It is possible to conduct HTTP request smuggling attacks by sending the Content-Length header twice. Furthermore, invalid Transfer Encoding headers were found to be parsed as valid which could be leveraged for TE:CL smuggling attacks.	7.5	More Details
CVE-2020-7670	agoo prior to 2.14.0 allows request smuggling attacks where agoo is used as a backend and a frontend proxy also being vulnerable. HTTP pipelining issues and request smuggling attacks might be possible due to incorrect Content-Length and Transfer encoding header parsing. It is possible to conduct HTTP request smuggling attacks where `agoo` is used as part of a chain of backend servers due to insufficient `Content-Length` and `Transfer Encoding` parsing.	7.5	More Details
CVE-2020-13270	Missing permission check on fork relation creation in GitLab CE/EE 11.3 and later through 13.0.1 allows guest users to create a fork relation on restricted public projects via API	7.5	More Details
CVE-2020-0181	In exif_data_load_data_thumbnail of exif-data.c, there is a possible denial of service due to an integer overflow. 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-145075076	7.5	More Details
CVE-2020-7502	A CWE-787: Out-of-bounds Write vulnerability exists in Modicon M218 Logic Controller (Firmware version 4.3 and prior), which may cause a Denial of Service when specific TCP/IP crafted packets are sent to the Modicon M218 Logic Controller.	7.5	More Details
CVE-2020-0534	Improper input validation in the DAL subsystem for Intel(R) CSME versions before 12.0.64, 13.0.32, 14.0.33 and 14.5.12 may allow an unauthenticated user to potentially enable denial of service via network access.	7.5	More Details
CVE-2020-0536	Improper input validation in the DAL subsystem for Intel(R) CSME versions before 11.8.77, 11.12.77, 11.22.77, 12.0.64, 13.0.32,14.0.33 and Intel(R) TXE versions before 3.1.75 and 4.0.25 may allow an unauthenticated user to potentially enable information disclosure via network access.	7.5	More Details
CVE-2020-0176	In avdt_msg_prs_rej of avdt_msg.cc, there is a possible out-of-bounds read due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-79702484	7.5	More Details
CVE-2020-0538	Improper input validation in subsystem for Intel(R) AMT versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable denial of service via network access.	7.5	More Details
CVE-2020-0540	Insufficiently protected credentials in Intel(R) AMT versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable information disclosure via network access.	7.5	More Details
CVE-2020-11090	In Indy Node 1.12.2, there is an Uncontrolled Resource Consumption vulnerability. Indy Node has a bug in TAA handling code. The current primary can be crashed with a malformed transaction from a client, which leads to a view change. Repeated rapid view changes have the potential of bringing down the network. This is fixed in version 1.12.3.	7.5	More Details
CVE-2020-0596	Improper input validation in DHCPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable information disclosure via network access.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0198	In exif_data_load_data_content of exif-data.c, there is a possible UBSAN abort due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146428941	7.5	More Details
CVE-2020-13900	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_sdp_preparse in sdp.c has a NULL pointer dereference.	7.5	More Details
CVE-2020-7506	A CWE-200: Information Exposure vulnerability exists in Easergy T300, Firmware V1.5.2 and prior, which could allow an attacker to pack or unpack the archive with the firmware for the controller and modules using the usual tar archiver resulting in an information exposure.	7.5	More Details
CVE-2020-4434	Certain IBM Aspera applications are vulnerable to buffer overflow based on the product configuration and valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180900.	7.5	More Details
CVE-2020-14048	Zoho ManageEngine ServiceDesk Plus before 11.1 build 11115 allows remote unauthenticated attackers to change the installation status of deployed agents.	7.5	More Details
CVE-2020-4045	SSB-DB version 20.0.0 has an information disclosure vulnerability. The get() method is supposed to only decrypt messages when you explicitly ask it to, but there is a bug where it's decrypting any message that it can. This means that it is returning the decrypted content of private messages, which a malicious peer could use to get access to private data. This only affects peers running SSB-DB@20.0.0 who also have private messages, and is only known to be exploitable if you're also running SSB-OOO (default in SSB-Server), which exposes a thin wrapper around get() to anonymous peers. This is fixed in version 20.0.1. Note that users of SSB-Server verion 16.0.0 should upgrade to 16.0.1 to get the fixed version of SSB-DB.	7.5	More Details
CVE-2020-13250	HashiCorp Consul and Consul Enterprise include an HTTP API (introduced in 1.2.0) and DNS (introduced in 1.4.3) caching feature that was vulnerable to denial of service. Fixed in 1.6.6 and 1.7.4.	7.5	More Details
CVE-2020-13170	HashiCorp Consul and Consul Enterprise did not appropriately enforce scope for local tokens issued by a primary data center, where replication to a secondary data center was not enabled. Introduced in 1.4.0, fixed in 1.6.6 and 1.7.4.	7.5	More Details
CVE-2020-12758	HashiCorp Consul and Consul Enterprise could crash when configured with an abnormally-formed service-router entry. Introduced in 1.6.0, fixed in 1.6.6 and 1.7.4.	7.5	More Details
CVE-2020-9643	Adobe Experience Manager versions 6.5 and earlier have a server-side request forgery (ssrf) vulnerability. Successful exploitation could lead to sensitive information disclosure.	7.5	More Details
CVE-2020-9645	Adobe Experience Manager versions 6.5 and earlier have a blind server-side request forgery (ssrf) vulnerability. Successful exploitation could lead to sensitive information disclosure.	7.5	More Details
CVE-2020-4432	Certain IBM Aspera applications are vulnerable to command injection after valid authentication, which could allow an attacker with intimate knowledge of the system to execute commands in a SOAP API. IBM X-Force ID: 180810.	7.5	More Details
CVE-2020-4433	Certain IBM Aspera applications are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker with intimate knowledge of the server to execute arbitrary code on the system with the privileges of root or cause server to crash. IBM X-Force ID: 180814.	7.5	More Details
CVE-2020-4435	Certain IBM Aspera applications are vulnerable to arbitrary memory corruption based on the product configuration, which could allow an attacker with intimate knowledge of the system to execute arbitrary code or perform a denial-of-service (DoS) through the http fallback service. IBM X-Force ID: 180901.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8543	OX App Suite through 7.10.3 has Improper Input Validation.	7.5	More Details
CVE-2020-4436	Certain IBM Aspera applications are vulnerable to buffer overflow after valid authentication, which could allow an attacker with intimate knowledge of the system to execute arbitrary code through a service. IBM X-Force ID: 180902.	7.5	More Details
CVE-2020-0214	In ce_t4t_process_select_file_cmd of ce_t4t.cc, there is a possible out of bounds read due to an incorrect 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-10Android ID: A-140292264	7.5	More Details
CVE-2020-9289	Use of a hard-coded cryptographic key to encrypt password data in CLI configuration in FortiManager 6.2.3 and below, FortiAnalyzer 6.2.3 and below may allow an attacker with access to the CLI configuration or the CLI backup file to decrypt the sensitive data, via knowledge of the hard-coded key.	7.5	More Details
CVE-2020-7513	A CWE-312: Cleartext Storage of Sensitive Information vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to intercept traffic and read configuration data.	7.5	More Details
CVE-2020-7511	A CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to acquire a password by brute force.	7.5	More Details
CVE-2020-6264	SAP Commerce, versions - 6.7, 1808, 1811, 1905, may allow an attacker to access information under certain conditions which would otherwise be restricted, leading to Information Disclosure.	7.5	More Details
CVE-2020-10752	A flaw was found in the OpenShift API Server, where it failed to sufficiently protect OAuthTokens by leaking them into the logs when an API Server panic occurred. This flaw allows an attacker with the ability to cause an API Server error to read the logs, and use the leaked OAuthToken to log into the API Server with the leaked token.	7.5	More Details
CVE-2020-7510	A CWE-200: Information Exposure vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow attacker to obtain private keys.	7.5	More Details
CVE-2020-7507	A CWE-400: Uncontrolled Resource Consumption vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to login multiple times resulting in a denial of service.	7.5	More Details
CVE-2020-0597	Out-of-bounds read in IPv6 subsystem in Intel(R) AMT and Intel(R) ISM versions before 14.0.33 may allow an unauthenticated user to potentially enable denial of service via network access.	7.5	More Details
CVE-2019-3617	Privilege escalation vulnerability in McAfee Total Protection (ToPS) for Mac OS prior to 4.6 allows local users to gain root privileges via incorrect protection of temporary files.	7.5	More Details
CVE-2020-0140	In rw_i93_sm_detect_ndef of rw_i93.c, there is a possible information disclosure 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-10Android ID: A-146053215	7.5	More Details
CVE-2020-4310	IBM MQ and MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 C are vulnerable to a denial of service attack due to an error within the Data Conversion logic. IBM X-Force ID: 177081.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10705	A flaw was discovered in Undertow in versions before Undertow 2.1.1.Final where certain requests to the "Expect: 100-continue" header may cause an out of memory error. This flaw may potentially lead to a denial of service.	7.5	More Details
CVE-2020-13223	HashiCorp Vault and Vault Enterprise logged proxy environment variables that potentially included sensitive credentials. Fixed in 1.3.6 and 1.4.2.	7.5	More Details
CVE-2020-13650	An issue was discovered in DigDash 2018R2 before p20200210 and 2019R1 before p20200210. The login page is vulnerable to Server-Side Request Forgery (SSRF) that allows use of the application as a proxy. Sent to an external server, a forged request discloses application credentials. For a request to an internal component, the request is blind, but through the error message it's possible to determine whether the request targeted a open service.	7.5	More Details
CVE-2020-12003	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. An exposed API call allows users to provide files to be processed without sanitation. This may allow an attacker to use specially crafted requests to traverse the file system and expose sensitive data on the local hard drive.	7.5	More Details
CVE-2020-0142	In rw_i93_sm_format of rw_i93.c, there is a possible information disclosure 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-10Android ID: A-146435761	7.5	More Details
CVE-2020-14149	In uftpd before 2.12, handle_CWD in ftpcmd.c mishandled the path provided by the user, causing a NULL pointer dereference and denial of service, as demonstrated by a CWD /.. command.	7.5	More Details
CVE-2020-14148	The Server-Server protocol implementation in ngIRCd before 26~rc2 allows an out-of-bounds access, as demonstrated by the IRC_NJOIN() function.	7.5	More Details
CVE-2019-20838	libpcre in PCRE before 8.43 allows a subject buffer over-read in JIT when UTF is disabled, and \X or \R has more than one fixed quantifier, a related issue to CVE-2019-20454.	7.5	More Details
CVE-2020-12005	FactoryTalk Linx versions 6.00, 6.10, and 6.11, RSLinx Classic v4.11.00 and prior,Connected Components Workbench: Version 12 and prior, ControlFLASH: Version 14 and later, ControlFLASH Plus: Version 1 and later, FactoryTalk Asset Centre: Version 9 and later, FactoryTalk Linx CommDTM: Version 1 and later, Studio 5000 Launcher: Version 31 and later Stud, 5000 Logix Designer software: Version 32 and prior is vulnerable. A vulnerability exists in the communication function that enables users to upload EDS files by FactoryTalk Linx. This may allow an attacker to upload a file with bad compression, consuming all the available CPU resources, leading to a denial-of-service condition.	7.5	More Details
CVE-2020-0128	In addPacket of AMPEG4ElementaryAssembler, there is an out of bounds read due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges required. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-123940919	7.5	More Details
CVE-2020-13238	Mitsubishi MELSEC iQ-R Series PLCs with firmware 33 allow attackers to halt the industrial process by sending an unauthenticated crafted packet over the network, because this denial of service attack consumes excessive CPU time. After halting, physical access to the PLC is required in order to restore production.	7.5	More Details
CVE-2020-12712	A vulnerability based on insecure user/password encryption in the JOE (job editor) component of SOS JobScheduler 1.12 and 1.13 allows attackers to decrypt the user/password that is optionally stored with a user's profile.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13898	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_sdp_process in sdp.c has a NULL pointer dereference.	7.5	More Details
CVE-2020-13850	Artica Pandora FMS 7.44 has inadequate access controls on a web folder.	7.5	More Details
CVE-2020-13899	An issue was discovered in janus-gateway (aka Janus WebRTC Server) through 0.10.0. janus_process_incoming_request in janus.c discloses information from uninitialized stack memory.	7.5	More Details
CVE-2020-4494	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow an attacker to bypass authentication due to improper session validation which can result in access to unauthorized resources. IBM X-Force ID: 182019.	7.5	More Details
CVE-2020-11622	A vulnerability exists in Arista's Cloud EOS VM / vEOS 4.23.2M and below releases in the 4.23.x train, 4.22.4M and below releases in the 4.22.x train, 4.21.3M to 4.21.9M releases in the 4.21.x train, 4.21.3FX-7368.*, 4.21.4-FCRFX.*, 4.21.4.1, 4.21.7.1, 4.22.2.0.1, 4.22.2.2.1, 4.22.3.1, and 4.23.2.1 Router code in a scenario where TCP MSS options are configured.	7.5	More Details
CVE-2020-14163	An issue was discovered in ecma/operations/ecma-container-object.c in JerryScript 2.2.0. Operations with key/value pairs did not consider the case where garbage collection is triggered after the key operation but before the value operation, as demonstrated by improper read access to memory in ecma_gc_set_object_visited in ecma/base/ecma-gc.c.	7.5	More Details
CVE-2020-4054	In Sanitize (RubyGem sanitize) greater than or equal to 3.0.0 and less than 5.2.1, there is a cross-site scripting vulnerability. When HTML is sanitized using Sanitize's "relaxed" config, or a custom config that allows certain elements, some content in a math or svg element may not be sanitized correctly even if math and svg are not in the allowlist. You are likely to be vulnerable to this issue if you use Sanitize's relaxed config or a custom config that allows one or more of the following HTML elements: iframe, math, noembed, noframes, noscript, plaintext, script, style, svg, xmp. Using carefully crafted input, an attacker may be able to sneak arbitrary HTML through Sanitize, potentially resulting in XSS (cross-site scripting) or other undesired behavior when that HTML is rendered in a browser. This has been fixed in 5.2.1.	7.3	More Details
CVE-2020-0133	In MockLocationAppPreferenceController.java, it is possible to mock the GPS location of the device due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145136060	7.3	More Details
CVE-2020-2028	An OS Command Injection vulnerability in PAN-OS management server allows authenticated administrators to execute arbitrary OS commands with root privileges when uploading a new certificate in FIPS-CC mode. This issue affects: All versions of PAN-OS 7.1 and PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.13; PAN-OS 9.0 versions earlier than PAN-OS 9.0.7.	7.2	More Details
CVE-2019-15123	The Branding Module in Viki Vera 4.9.1.26180 allows an authenticated user to change the logo on the website. An attacker could use this to upload a malicious .aspx file and gain Remote Code Execution on the site.	7.2	More Details
CVE-2020-12713	An issue was discovered in CipherMail Community Gateway and Professional/Enterprise Gateway 1.0.1 through 4.7.1-0 and CipherMail Webmail Messenger 1.1.1 through 3.1.1-0. Attackers with administrative access to the web interface have multiple options to escalate their privileges to the Unix root account.	7.2	More Details
CVE-2020-7509	A CWE-269: Improper privilege management (write) vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to elevate their privileges and delete files.	7.2	More Details
CVE-2020-7505	A CWE-494 Download of Code Without Integrity Check vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to inject data with dangerous content into the firmware and execute arbitrary code on the system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2027	A buffer overflow vulnerability in the authd component of the PAN-OS management server allows authenticated administrators to disrupt system processes and potentially execute arbitrary code with root privileges. This issue affects: All versions of PAN-OS 7.1 and PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.13; PAN-OS 9.0 versions earlier than PAN-OS 9.0.7.	7.2	More Details
CVE-2020-2029	An OS Command Injection vulnerability in the PAN-OS web management interface allows authenticated administrators to execute arbitrary OS commands with root privileges by sending a malicious request to generate new certificates for use in the PAN-OS configuration. This issue affects: All versions of PAN-OS 8.0; PAN-OS 7.1 versions earlier than PAN-OS 7.1.26; PAN-OS 8.1 versions earlier than PAN-OS 8.1.13.	7.2	More Details
CVE-2020-13855	Artica Pandora FMS 7.44 allows arbitrary file upload (leading to remote command execution) via the File Repository Manager feature.	7.2	More Details
CVE-2020-13852	Artica Pandora FMS 7.44 allows arbitrary file upload (leading to remote command execution) via the File Manager feature.	7.2	More Details
CVE-2020-12725	Havoc Research discovered an authenticated Server-Side Request Forgery (SSRF) via the "JSON" data source of Redash open-source 8.0.0 and prior. Possibly, other connectors are affected. The SSRF is potent and provides a lot of flexibility in terms of being able to craft HTTP requests e.g., by adding headers, selecting any HTTP verb, etc.	7.2	More Details
CVE-2020-6090	An exploitable code execution vulnerability exists in the Web-Based Management (WBM) functionality of WAGO PFC 200 03.03.10(15). A specially crafted series of HTTP requests can cause code execution resulting in remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	7.2	More Details
CVE-2020-0532	Improper input validation in subsystem for Intel(R) AMT versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access.	7.1	More Details
CVE-2020-5362	Dell Client Consumer and Commercial platforms include an improper authorization vulnerability in the Dell Manageability interface for which an unauthorized actor, with local system access with OS administrator privileges, could bypass the BIOS Administrator authentication to restore BIOS Setup configuration to default values.	7.1	More Details
CVE-2020-14153	In IJG JPEG (aka libjpeg) from version 8 through 9c, jdhuff.c has an out-of-bounds array read for certain table pointers.	7.1	More Details
CVE-2020-14152	In IJG JPEG (aka libjpeg) before 9d, jpeg_mem_available() in jmemnobs.c in djpeg does not honor the max_memory_to_use setting, possibly causing excessive memory consumption.	7.1	More Details
CVE-2020-0218	In loadSoundModel and related functions of SoundTriggerHwService.cpp, there is possible out of bounds write due to a race condition. 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-136005905	7.0	More Details
CVE-2020-12850	The following vulnerability applies only to the Pydio Cells Enterprise OVF version 2.0.4. Prior versions of the Pydio Cells Enterprise OVF (such as version 2.0.3) have a looser policy restriction allowing the “pydio” user to execute any privileged command using sudo. In version 2.0.4 of the appliance, the user pydio is responsible for running all the services and binaries that are contained in the Pydio Cells web application package, such as mysqld, cells, among others. This user has privileges restricted to run those services and nothing more.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2032	A race condition vulnerability Palo Alto Networks GlobalProtect app on Windows allows a local limited Windows user to execute programs with SYSTEM privileges. This issue can be exploited only while performing a GlobalProtect app upgrade. This issue affects: GlobalProtect app 5.0 versions earlier than GlobalProtect app 5.0.10 on Windows; GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.4 on Windows.	7.0	More Details
CVE-2020-0204	In InstallPackage of package.cpp, there is a possible bypass of a signature check due to a Time of Check/Time of Use condition. This could lead to local escalation of privilege by allowing a bypass of the initial zip file signature check for an OS update with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-136498130	7.0	More Details
CVE-2020-13162	A time-of-check time-of-use vulnerability in PulseSecureService.exe in Pulse Secure Client versions prior to 9.1.6 down to 5.3 R70 for Windows (which runs as NT AUTHORITY/SYSTEM) allows unprivileged users to run a Microsoft Installer executable with elevated privileges.	7.0	More Details
CVE-2019-3585	Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 14 may allow local users to interact with the On-Access Scan Messages - Threat Alert Window with elevated privileges via running McAfee Tray with elevated privileges.	7.0	More Details
CVE-2020-4047	In affected versions of WordPress, authenticated users with upload permissions (like authors) are able to inject JavaScript into some media file attachment pages in a certain way. This can lead to script execution in the context of a higher privileged user when the file is viewed by them. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).	6.8	More Details
CVE-2020-0566	Improper Access Control in subsystem for Intel(R) TXE versions before 3.175 and 4.0.25 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2020-8675	Insufficient control flow management in firmware build and signing tool for Intel(R) Innovation Engine before version 1.0.859 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2020-9076	HUAWEI P30;HUAWEI P30 Pro;Tony-AL00B smartphones with versions earlier than 10.1.0.135(C00E135R2P11); versions earlier than 10.1.0.135(C00E135R2P8), versions earlier than 10.1.0.135 have an improper authentication vulnerability. Due to the identity of the message sender not being properly verified, an attacker can exploit this vulnerability through man-in-the-middle attack to induce user to access malicious URL.	6.8	More Details
CVE-2020-1813	HUAWEI P30 smart phone with versions earlier than 10.1.0.135(C00E135R2P11) have an improper authentication vulnerability. Due to improper authentication of specific interface, in specific scenario attackers could access specific interface without authentication. Successful exploit could allow the attacker to perform unauthorized operations.	6.8	More Details
CVE-2020-0165	In phNxpNciHal_NfcDep_cmd_ext of phNxpNciHal_NfcDepSWPrio.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139532977	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7580	A vulnerability has been identified in SIMATIC Automation Tool (All versions < V4 SP2), 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 Upd3), SIMATIC PCS neo (All versions < V3.0 SP1), SIMATIC ProSave (All versions < V17), SIMATIC S7-1500 Software Controller (All versions < V21.8), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2 Update 4), SIMATIC STEP 7 (TIA Portal) V14 (All versions < V14 SP1 Update 10), SIMATIC STEP 7 (TIA Portal) V15 (All versions < V15.1 Update 5), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMATIC STEP 7 V5 (All versions < V5.6 SP2 HF3), SIMATIC WinCC OA V3.16 (All versions < V3.16 P018), SIMATIC WinCC OA V3.17 (All versions < V3.17 P003), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 2), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2 Update 4), SIMATIC WinCC Runtime Professional V14 (All versions < V14 SP1 Update 10), SIMATIC WinCC Runtime Professional V15 (All versions < V15.1 Update 5), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER (All Versions < V5.4 HF2), SINAMICS Startdrive (All Versions < V16 Update 3), SINEC NMS (All versions < V1.0 SP2), SINEMA Server (All versions < V14 SP3), SINUMERIK ONE virtual (All Versions < V6.14), SINUMERIK Operate (All Versions < V6.14). A common component used by the affected applications regularly calls a helper binary with SYSTEM privileges while the call path is not quoted. This could allow a local attacker to execute arbitrary code with SYTEM privileges.	6.7	More Details
CVE-2020-0124	In markBootComplete of InstalldNativeService.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-140237592	6.7	More Details
CVE-2020-0186	In hal_fd_init of hal_fd.cc, there is a possible out of bounds write due to an incorrect 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-146144463	6.7	More Details
CVE-2020-0533	Reversible one-way hash in Intel(R) CSME versions before 11.8.76, 11.12.77 and 11.22.77 may allow a privileged user to potentially enable escalation of privilege, denial of service or information disclosure via local access.	6.7	More Details
CVE-2020-0153	In phNxpNciHal_write_ext of phNxpNciHal_ext.cc, 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-139733543	6.7	More Details
CVE-2020-5358	Dell Encryption versions prior to 10.7 and Dell Endpoint Security Suite versions prior to 2.7 contain a privilege escalation vulnerability due to incorrect permissions. A local malicious user with low privileges could potentially exploit this vulnerability to gain elevated privilege on the affected system with the help of a symbolic link.	6.7	More Details
CVE-2020-0541	Out-of-bounds write in subsystem for Intel(R) CSME versions before 12.0.64, 13.0.32, 14.0.33 and 14.5.12 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-4471	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow an unauthenticated attacker to cause a denial of service or hijack DNS sessions by send a specially crafted HTTP command to the remote server. IBM X-Force ID: 181726.	6.5	More Details
CVE-2020-4477	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 discloses highly sensitive information in plain text in the virgo log file which could be used in further attacks against the system. IBM X-Force ID: 181779.	6.5	More Details
CVE-2020-8544	OX App Suite through 7.10.3 allows SSRF.	6.5	More Details
CVE-2020-4320	IBM MQ Appliance and IBM MQ AMQP Channels 8.0, 9.0 LTS, 9.1 LTS, and 9.1 CD do not correctly block or allow clients based on the certificate distinguished name SSLPEER setting. IBM X-Force ID: 177403.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1825	FusionAccess with versions earlier than 6.5.1.SPC002 have a Denial of Service (DoS) vulnerability. Due to insufficient verification on specific input, attackers can exploit this vulnerability by sending constructed messages to the affected device through another device on the same network. Successful exploit could cause affected devices to be abnormal.	6.5	More Details
CVE-2020-14199	BIP-143 in the Bitcoin protocol specification mishandles the signing of a Segwit transaction, which allows attackers to trick a user into making two signatures in certain cases, potentially leading to a huge transaction fee. NOTE: this affects all hardware wallets. It was fixed in 1.9.1 for the Trezor One and 2.3.1 for the Trezor Model T.	6.5	More Details
CVE-2018-16848	A Denial of Service (DoS) condition is possible in OpenStack Mistral in versions up to and including 7.0.3. Submitting a specially crafted workflow definition YAML file containing nested anchors can lead to resource exhaustion culminating in a denial of service.	6.5	More Details
CVE-2020-7499	A CWE-863: Incorrect Authorization vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes.	6.5	More Details
CVE-2020-9075	Huawei products Secospace USG6300;USG6300E with versions of V500R001C30,V500R001C50,V500R001C60,V500R001C80,V500R005C00,V500R005C10;V600R006C00 have a vulnerability of insufficient input verification. An attacker with limited privilege can exploit this vulnerability to access a specific directory. Successful exploitation of this vulnerability may lead to information leakage.	6.5	More Details
CVE-2020-0531	Improper input validation in Intel(R) AMT versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow an authenticated user to potentially enable information disclosure via network access.	6.5	More Details
CVE-2020-7492	A CWE-521: Weak Password Requirements vulnerability exists in the GP-Pro EX V1.00 to V4.09.100 which could cause the discovery of the password when the user is entering the password because it is not masqueraded.	6.5	More Details
CVE-2020-8541	OX App Suite through 7.10.3 allows XXE attacks.	6.5	More Details
CVE-2020-0212	In _onBufferDestroyed of InputBufferManager.cpp, there is a possible out of bounds read due to a use after free. 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-135140854	6.5	More Details
CVE-2020-14214	Zammad before 3.3.1, when Domain Based Assignment is enabled, relies on a claimed e-mail address for authorization decisions. An attacker can register a new account that will have access to all tickets of an arbitrary Organization.	6.5	More Details
CVE-2020-0175	In XMF_ReadNode of eas_xmf.c, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-126380818	6.5	More Details
CVE-2020-0205	In the DaalaBitReader constructor of entropy_decoder.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure in the media server with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-147234020	6.5	More Details
CVE-2020-0200	In ReadLittleEndian of raw_bit_reader.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure in the media server with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-147231862	6.5	More Details
CVE-2020-0161	In parseChunk of MPEG4Extractor.cpp, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127973550	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0196	In RegisterNotificationResponse::GetEvent of register_notification_packet.cc, there is a possible abort due to improper input validation. This could lead to remote denial of service of the Bluetooth service, over Bluetooth, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-144066833	6.5	More Details
CVE-2020-0195	In ihevcd_iquant_itrans_recon_ctb of ihevcd_iquant_itrans_recon_ctb.c and related functions, 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-144686961	6.5	More Details
CVE-2020-0193	In ihevc_intra_pred_chroma_mode_3_to_9_av8 of ihevc_intra_pred_chroma_mode_3_to_9.s, there is a possible out of bounds read due to a heap buffer overflow. 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-144595488	6.5	More Details
CVE-2020-0192	In ih264d_decode_slice_thread of ih264d_thread_parse_decode.c, there is a possible out of bounds read due to improper input validation. 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-144687080	6.5	More Details
CVE-2020-0162	In parseSampleAuxiliaryInformationOffsets of MPEG4Extractor.cpp, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-124526959	6.5	More Details
CVE-2020-0191	In ih264d_update_default_index_list() of ih264d_dpb_mgr.c, there is a possible out of bounds read due to a logic error. 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-140561484	6.5	More Details
CVE-2020-0189	In ihevcd_decode() of ihevcd_decode.c, there is possible resource exhaustion due to an infinite loop. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139939283	6.5	More Details
CVE-2020-0163	In parseSampleAuxiliaryInformationSizes of MPEG4Extractor.cpp, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-124525515	6.5	More Details
CVE-2020-0169	In RTTTL_Event of eas_rtttl.c, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-123700383	6.5	More Details
CVE-2020-0170	In IMY_Event of eas_imelody.c, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127310810	6.5	More Details
CVE-2020-0171	In Parse_lart of eas_mdls.c, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127313223	6.5	More Details
CVE-2020-0172	In Parse_art of eas_mdls.c, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127312550	6.5	More Details
CVE-2020-0173	In Parse_lins of eas_mdls.c, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127313764	6.5	More Details
CVE-2020-0184	In ihevcd_ref_list() of ihevcd_ref_list.c, there is a possible infinite loop due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141688974	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0182	In exif_entry_get_value of exif-entry.c, 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-147140917	6.5	More Details
CVE-2020-0180	In GetOpusHeaderBuffers() of OpusHeader.cpp, there is a possible out of bounds read due to a missing bounds check. 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-142861738	6.5	More Details
CVE-2020-0127	In AudioStream::decode of AudioGroup.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure in the phone process with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140054506	6.5	More Details
CVE-2020-0174	In Parse_ptbl of eas_mdls.c, there is possible resource exhaustion due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127313537	6.5	More Details
CVE-2020-0207	In next_marker of jdmarker.c, there is a possible out of bounds read due to improper input validation. 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-135532289	6.5	More Details
CVE-2020-10755	An insecure-credentials flaw was found in all openstack-cinder versions before openstack-cinder 14.1.0, all openstack-cinder 15.x.x versions before openstack-cinder 15.2.0 and all openstack-cinder 16.x.x versions before openstack-cinder 16.1.0. When using openstack-cinder with the Dell EMC ScaleIO or VxFlex OS backend storage driver, credentials for the entire backend are exposed in the ``connection_info`` element in all Block Storage v3 Attachments API calls containing that element. This flaw enables an end-user to create a volume, make an API call to show the attachment detail information, and retrieve a username and password that may be used to connect to another user's volume. Additionally, these credentials are valid for the ScaleIO or VxFlex OS Management API, should an attacker discover the Management API endpoint. Source: OpenStack project	6.5	More Details
CVE-2020-6269	Under certain conditions SAP Business Objects Business Intelligence Platform, version 4.2, allows an attacker to access information which would otherwise be restricted, leading to Information Disclosure.	6.5	More Details
CVE-2020-6270	SAP NetWeaver AS ABAP (Banking Services), versions - 710, 711, 740, 750, 751, 752, 75A, 75B, 75C, 75D, 75E, does not perform necessary authorization checks for an authenticated user due to Missing Authorization Check, allowing wrong and unexpected change of individual conditions by a malicious user leading to wrong prices.	6.5	More Details
CVE-2020-0211	In SumCompoundHorizontalTaps of convolve_neon.cc, there is a possible out of bounds read due to a missing bounds check. 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-147491773	6.5	More Details
CVE-2020-13444	Liferay Portal 7.x before 7.3.2, and Liferay DXP 7.0 before fix pack 92, 7.1 before fix pack 18, and 7.2 before fix pack 5 does not sanitize the information returned by the DDMDataProvider API, which allows remote authenticated users to obtain the password to REST Data Providers.	6.5	More Details
CVE-2020-0213	In hevcd_fmt_conv_420sp_to_420sp_av8 of ihevcd_fmt_conv_420sp_to_420sp.s, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-10 Android-11 Android ID: A-143464314	6.5	More Details
CVE-2020-0126	In multiple functions in DrmPlugin.cpp, there is a possible use after free due to a race condition. This could lead to local code execution with System execution privileges required. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-137878930	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11980	In Karaf, JMX authentication takes place using JAAS and authorization takes place using ACL files. By default, only an "admin" can actually invoke on an MBean. However there is a vulnerability there for someone who is not an admin, but has a "viewer" role. In the 'etc/jmx.acl.cfg', such as role can call get*. It's possible to authenticate as a viewer role + invokes on the MLet getMBeansFromURL method, which goes off to a remote server to fetch the desired MBean, which is then registered in Karaf. At this point the attack fails as "viewer" doesn't have the permission to invoke on the MBean. Still, it could act as a SSRF style attack and also it essentially allows a "viewer" role to pollute the MBean registry, which is a kind of privilege escalation. The vulnerability is low as it's possible to add a ACL to limit access. Users should update to Apache Karaf 4.2.9 or newer.	6.3	More Details
CVE-2020-4052	In Wiki.js before 2.4.107, there is a stored cross-site scripting through template injection. This vulnerability exists due to an insecure validation mechanism intended to insert v-pre tags into rendered HTML elements which contain curly-braces. By creating a crafted wiki page, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the page is viewed by other users. This has been patched in 2.4.107.	6.3	More Details
CVE-2019-3588	Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 14 may allow unauthorized users to interact with the On-Access Scan Messages - Threat Alert Window when the Windows Login Screen is locked.	6.3	More Details
CVE-2020-3928	GeoVision Door Access Control device family is hardcoded with a root password, which adopting an identical password in all devices.	6.2	More Details
CVE-2020-10268	Critical services for operation can be terminated from windows task manager, bringing the manipulator to a halt. After this a Re-Calibration of the brakes needs to be performed. Be noted that this only can be accomplished either by a Kuka technician or by Kuka issued calibration hardware that interfaces with the manipulator furthering the delay and increasing operational costs.	6.1	More Details
CVE-2020-9522	Cross Site Scripting (XSS) vulnerability in Micro Focus ArcSight Enterprise Security Manager (ESM) product, Affecting versions 7.0.x, 7.2 and 7.2.1 . The vulnerabilities could be remotely exploited resulting in Cross-Site Scripting (XSS) or information disclosure.	6.1	More Details
CVE-2020-14010	The Laborator Xenon theme 1.3 for WordPress allows Reflected XSS via the data/typeahead-generate.php q (aka name) parameter.	6.1	More Details
CVE-2020-5592	Cross-site scripting vulnerability in Zenphoto versions prior to 1.5.7 allows remote attackers to inject an arbitrary JavaScript via unspecified vectors.	6.1	More Details
CVE-2020-13269	A Reflected Cross-Site Scripting vulnerability allowed the execution of arbitrary Javascript code on the Static Site Editor in GitLab CE/EE 12.10 and later through 13.0.1	6.1	More Details
CVE-2020-13267	A Stored Cross-Site Scripting vulnerability allowed the execution on Javascript payloads on the Metrics Dashboard in GitLab CE/EE 12.8 and later through 13.0.1	6.1	More Details
CVE-2020-13652	An issue was discovered in DigDash 2018R2 before p20200528, 2019R1 before p20200528, 2019R2 before p20200430, and 2020R1 before p20200507. A cross-site scripting (XSS) vulnerability exists in the login menu.	6.1	More Details
CVE-2020-6246	SAP NetWeaver AS ABAP Business Server Pages Test Application SBSPEXT_TABLE, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, does not sufficiently encode user-controlled inputs, resulting in reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2020-14210	Reflected Cross-Site Scripting (XSS) vulnerability in MONITORAPP WAF in which script can be executed when responding to Request URL information. It provides a function to response to Request URL information when blocking.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13271	A Stored Cross-Site Scripting vulnerability allowed the execution of arbitrary Javascript code in the blobs API in all previous GitLab CE/EE versions through 13.0.1	6.1	More Details
CVE-2020-9426	OX Guard 2.10.3 and earlier allows XSS.	6.1	More Details
CVE-2020-11839	Cross Site Scripting (XSS) vulnerability in Micro Focus ArcSight Logger product, affecting all version from 6.6.1 up to version 7.0.1. The vulnerabilities could be remotely exploited resulting in Cross-Site Scripting (XSS) or information disclosure.	6.1	More Details
CVE-2020-9648	Adobe Experience Manager versions 6.5 and earlier have a cross-site scripting vulnerability. Successful exploitation could lead to arbitrary javascript execution in the browser.	6.1	More Details
CVE-2019-19112	The wpForo plugin 1.6.5 for WordPress allows XSS involving the wpf-dw-td-value class of dashboard.php.	6.1	More Details
CVE-2020-9651	Adobe Experience Manager versions 6.5 and earlier have a cross-site scripting (reflected) vulnerability. Successful exploitation could lead to arbitrary javascript execution in the browser.	6.1	More Details
CVE-2019-19111	The wpForo plugin 1.6.5 for WordPress allows XSS via the wp-admin/admin.php?page=wpforo-phrases langid parameter.	6.1	More Details
CVE-2020-9647	Adobe Experience Manager versions 6.5 and earlier have a cross-site scripting (dom-based) vulnerability. Successful exploitation could lead to arbitrary javascript execution in the browser.	6.1	More Details
CVE-2019-3613	DLL Search Order Hijacking vulnerability in McAfee Agent (MA) prior to 5.6.4 allows attackers with local access to execute arbitrary code via execution from a compromised folder.	5.9	More Details
CVE-2020-3929	GeoVision Door Access Control device family employs shared cryptographic private keys for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages.	5.9	More Details
CVE-2020-14093	Mutt before 1.14.3 allows an IMAP fcc/postpone man-in-the-middle attack via a PREAUTH response.	5.9	More Details
CVE-2020-12714	An issue was discovered in CipherMail Community Gateway Virtual Appliances and Professional/Enterprise Gateway Virtual Appliances versions 1.0.1 through 4.7.1-0 and CipherMail Webmail Messenger Virtual Appliances 1.1.1 through 3.1.1-0. A Diffie-Hellman parameter of insufficient size could allow man-in-the-middle compromise of communications between CipherMail products and external SMTP clients.	5.9	More Details
CVE-2019-16252	Missing SSL Certificate Validation in the Nutfind.com application through 3.9.12 for Android allows a man-in-the-middle attacker to sniff and manipulate all API requests, including login credentials and location data.	5.9	More Details
CVE-2020-4048	In affected versions of WordPress, due to an issue in wp_validate_redirect() and URL sanitization, an arbitrary external link can be crafted leading to unintended/open redirect when clicked. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0206	In the settings app, there is a possible app crash due to improper input validation. This could lead to local denial of service of the Settings app with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-136005061	5.5	More Details
CVE-2020-14150	GNU Bison before 3.5.4 allows attackers to cause a denial of service (application crash). NOTE: there is a risk only if Bison is used with untrusted input, and an observed bug happens to cause unsafe behavior with a specific compiler/architecture. The bug reports were intended to show that a crash may occur in Bison itself, not that a crash may occur in code that is generated by Bison.	5.5	More Details
CVE-2020-0134	In BnDrm::onTransact of IDrm.cpp, there is a possible information disclosure 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-146052771	5.5	More Details
CVE-2020-0132	In BnAAudioService::onTransact of IAAudioService.cpp, there is a possible out of bounds read due to unsafe deserialization. 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-139473816	5.5	More Details
CVE-2020-0121	In updateUidProcState of AppOpsService.java, there is a possible permission bypass due to a logic error. This could lead to local information disclosure of location data with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-148180766	5.5	More Details
CVE-2020-7495	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability during zip file extraction exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD) which could cause unauthorized write access outside of expected path folder when opening the project file.	5.5	More Details
CVE-2020-0156	In NxpNfc::ioctl of NxpNfc.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139736127	5.5	More Details
CVE-2020-0116	In checkSystemLocationAccess of LocationAccessPolicy.java, there is a possible bypass of user profile isolation due to a permissions bypass. 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-151330809	5.5	More Details
CVE-2020-0113	In sendCaptureResult of Camera3OutputUtils.cpp, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-9Android ID: A-150944913	5.5	More Details
CVE-2020-13999	ScaleViewPortExtEx in libemf.cpp in libEMF (aka ECMA-234 Metafile Library) 1.0.12 allows an integer overflow and denial of service via a crafted EMF file.	5.5	More Details
CVE-2020-0177	In connect() of PanService.java, there is a possible permissions bypass. This could lead to local escalation of privilege to change network connection settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-126206353	5.5	More Details
CVE-2020-0185	In avrc_pars_browsing_cmd of avrc_pars_tg.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-79945152	5.5	More Details
CVE-2020-0178	In getAllConfigFlags of SettingsProvider.cpp, there is a possible illegal read due to a missing permission check. This could lead to local information disclosure of config flags with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143299398	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0197	In InitDataParser::parsePssh of InitDataParser.cpp, 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-137370379	5.5	More Details
CVE-2020-0167	In load of ResourceTypes.cpp, there is a possible out of bounds read due to an integer overflow. 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-129475100	5.5	More Details
CVE-2020-0159	In rw_mfc_writeBlock of rw_mfc.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 needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140768035	5.5	More Details
CVE-2020-0543	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-0187	In engineSetMode of BaseBlockCipher.java, there is a possible incorrect cryptographic algorithm chosen due to an incomplete comparison. 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-148517383	5.5	More Details
CVE-2020-0539	Path traversal in subsystem for Intel(R) DAL software for Intel(R) CSME versions before 11.8.77, 11.12.77, 11.22.77, 12.0.64, 13.0.32, 14.0.33 and Intel(R) TXE versions before 3.1.75, 4.0.25 may allow an unprivileged user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-4406	IBM Spectrum Protect Client 8.1.7.0 through 8.1.9.1 (Linux and Windows), 8.1.9.0 trough 8.1.9.1 (AIX) and IBM Spectrum Protect for Space Management 8.1.7.0 through 8.1.9.1 (Linux), 8.1.9.0 through 8.1.9.1 (AIX) web user interfaces could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 179488.	5.4	More Details
CVE-2020-14012	scp/categories.php in osTicket 1.14.2 allows XSS via a Knowledgebase Category Name or Category Description. The attacker must be an Agent.	5.4	More Details
CVE-2020-13853	Artica Pandora FMS 7.44 has persistent XSS in the Messages feature.	5.4	More Details
CVE-2020-8542	OX App Suite through 7.10.3 allows XSS.	5.4	More Details
CVE-2020-4380	IBM Workload Scheduler 9.3.0.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 179160.	5.4	More Details
CVE-2020-14146	KumbiaPHP through 1.1.1, in Development mode, allows XSS via the public/pages/kumbia PATH_INFO.	5.4	More Details
CVE-2020-4046	In affected versions of WordPress, users with low privileges (like contributors and authors) can use the embed block in a certain way to inject unfiltered HTML in the block editor. When affected posts are viewed by a higher privileged user, this could lead to script execution in the editor/wp-admin. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11838	Cross Site Scripting (XSS) vulnerability in Micro Focus ArcSight Management Center product, Affecting versions 2.6.1, 2.7.x, 2.8.x, 2.9.x prior to 2.9.4. The vulnerabilities could be remotely exploited resulting in Cross-Site Scripting (XSS) or information disclosure.	5.4	More Details
CVE-2020-14213	In Zammad before 3.3.1, a Customer has ticket access that should only be available to an Agent (e.g., read internal data, split, or merge).	5.4	More Details
CVE-2020-4251	IBM API Connect 5.0.0.0 through 5.0.8.8 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: 175489.	5.4	More Details
CVE-2020-9644	Adobe Experience Manager versions 6.5 and earlier have a cross-site scripting (stored) vulnerability. Successful exploitation could lead to arbitrary javascript execution in the browser.	5.4	More Details
CVE-2020-6266	SAP Fiori for SAP S/4HANA, versions - 100, 200, 300, 400, allows an attacker to redirect users to a malicious site due to insufficient URL validation, leading to URL Redirection.	5.4	More Details
CVE-2020-14155	libpcre in PCRE before 8.44 allows an integer overflow via a large number after a (?C substring.	5.3	More Details
CVE-2020-11798	A Directory Traversal vulnerability in the web conference component of Mitel MiCollab AWV before 8.1.2.4 and 9.x before 9.1.3 could allow an attacker to access arbitrary files from restricted directories of the server via a crafted URL, due to insufficient access validation. A successful exploit could allow an attacker to access sensitive information from the restricted directories.	5.3	More Details
CVE-2020-13998	Citrix XenApp 6.5, when 2FA is enabled, allows a remote unauthenticated attacker to ascertain whether a user exists on the server, because the 2FA error page only occurs after a valid username is entered. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.3	More Details
CVE-2020-0535	Improper input validation in Intel(R) AMT versions before 11.8.76, 11.12.77, 11.22.77 and 12.0.64 may allow an unauthenticated user to potentially enable information disclosure via network access.	5.3	More Details
CVE-2020-12797	HashiCorp Consul and Consul Enterprise failed to enforce changes to legacy ACL token rules due to non-propagation to secondary data centers. Introduced in 1.4.0, fixed in 1.6.6 and 1.7.4.	5.3	More Details
CVE-2019-17655	A cleartext storage in a file or on disk (CWE-313) vulnerability in FortiOS SSL VPN 6.2.0 through 6.2.2, 6.0.9 and earlier and FortiProxy 2.0.0, 1.2.9 and earlier may allow an attacker to retrieve a logged-in SSL VPN user's credentials should that attacker be able to read the session file stored on the targeted device's system.	5.3	More Details
CVE-2020-2033	When the pre-logon feature is enabled, a missing certification validation in Palo Alto Networks GlobalProtect app can disclose the pre-logon authentication cookie to a man-in-the-middle attacker on the same local area network segment with the ability to manipulate ARP or to conduct ARP spoofing attacks. This allows the attacker to access the GlobalProtect Server as allowed by configured Security rules for the 'pre-login' user. This access may be limited compared to the network access of regular users. This issue affects: GlobalProtect app 5.0 versions earlier than GlobalProtect app 5.0.10 when the prelogon feature is enabled; GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.4 when the prelogon feature is enabled.	5.3	More Details
CVE-2020-6260	SAP Solution Manager (Trace Analysis), version 7.20, allows an attacker to inject superflous data that can be displayed by the application, due to Incomplete XML Validation. The application shows additional data that do not actually exist.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8674	Out-of-bounds read in DHCPv6 subsystem in Intel(R) AMT and Intel(R)ISM versions before 11.8.77, 11.12.77, 11.22.77, 12.0.64 and 14.0.33 may allow an unauthenticated user to potentially enable information disclosure via network access.	5.3	More Details
CVE-2020-0119	In addOrUpdateNetworkInternal and related functions of WifiConfigManager.java, there is a possible man in the middle attack due to improper certificate validation. 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-150500247	5.3	More Details
CVE-2020-7504	A CWE-20: Improper Input Validation vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to disable the webserver service on the device when specially crafted network packets are sent.	5.3	More Details
CVE-2020-13268	A specially crafted request could be used to confirm the existence of files hosted on object storage services, without disclosing their contents. This vulnerability affects GitLab CE/EE 12.10 and later through 13.0.1	5.3	More Details
CVE-2020-12494	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device.	5.3	More Details
CVE-2020-9427	OX Guard 2.10.3 and earlier allows SSRF.	5.0	More Details
CVE-2020-0157	In nfa_hci_conn_cback of nfa_hci_main.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139740814	4.9	More Details
CVE-2020-0537	Improper input validation in subsystem for Intel(R) AMT versions before 11.8.77, 11.12.77, 11.22.77 and 12.0.64 may allow a privileged user to potentially enable denial of service via network access.	4.9	More Details
CVE-2020-14154	Mutt before 1.14.3 proceeds with a connection even if, in response to a GnuTLS certificate prompt, the user rejects an expired intermediate certificate.	4.8	More Details
CVE-2019-19110	The wpForo plugin 1.6.5 for WordPress allows XSS via the wp-admin/admin.php?page=wpforo-phrases s parameter.	4.8	More Details
CVE-2020-7279	DLL Search Order Hijacking Vulnerability in the installer component of McAfee Host Intrusion Prevention System (Host IPS) for Windows prior to 8.0.0 Patch 15 Update allows attackers with local access to execute arbitrary code via execution from a compromised folder.	4.6	More Details
CVE-2020-12023	Philips IntelliBridge Enterprise (IBE), Versions B.12 and prior, IntelliBridge Enterprise system integration with SureSigns (VS4), EarlyVue (VS30) and IntelliVue Guardian (IGS). Unencrypted user credentials received in the IntelliBridge Enterprise (IBE) are logged within the transaction logs, which are secured behind the login based administrative web portal. The unencrypted user credentials sent from the affected products listed above, for the purpose of handshake or authentication with the Enterprise Systems, are logged as the payload in IntelliBridge Enterprise (IBE) within the transaction logs. An attacker with administrative privileges could exploit this vulnerability to read plain text credentials from log files.	4.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0144	In btm_proc_sp_req_evt of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142543497	4.4	More Details
CVE-2020-6239	Under certain conditions SAP Business One (Backup service), versions 9.3, 10.0, allows an attacker with admin permissions to view SYSTEM user password in clear text, leading to Information Disclosure.	4.4	More Details
CVE-2020-0149	In btu_hcif_mode_change_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 via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142544089	4.4	More Details
CVE-2020-0147	In btu_hcif_esco_connection_chg_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 via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142638392	4.4	More Details
CVE-2020-0146	In btu_hcif_hardware_error_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 via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142546561	4.4	More Details
CVE-2020-0145	In btm_simple_pair_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142544079	4.4	More Details
CVE-2020-0143	In nfa_dm_ndef_find_next_handler of nfa_dm_ndef.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure of heap data via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145597277	4.4	More Details
CVE-2020-0141	In OutputBuffersArray::realloc of CCodecBuffers.cpp, there is a possible heap disclosure due to a race condition. This could lead to remote information disclosure with System execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142544793	4.4	More Details
CVE-2020-0151	In avb_vbmeta_image_verify of avb_vbmeta_image.c there is a possible out of bounds read due to a missing bounds check. This could lead to a local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-133164384	4.4	More Details
CVE-2020-0545	Integer overflow in subsystem for Intel(R) CSME versions before 11.8.77, 11.12.77, 11.22.77 and Intel(R) TXE versions before 3.1.75, 4.0.25 and Intel(R) Server Platform Services (SPS) versions before SPS_E5_04.01.04.380.0, SPS_SoC-X_04.00.04.128.0, SPS_SoC-A_04.00.04.211.0, SPS_E3_04.01.04.109.0, SPS_E3_04.08.04.070.0 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-0139	In NDEF_MsgValidate of ndef_utils.c, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure if a malformed NFC tag is provided by the firmware. System execution privileges are needed and user interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145520471	4.4	More Details
CVE-2020-0527	Insufficient control flow management in firmware for some Intel(R) Data Center SSDs may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0135	In dump of RollbackManagerServiceImpl.java, there is a possible backup metadata exposure due to a missing permission 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-150949837	4.4	More Details
CVE-2020-0164	In phNxpNciHal_NfcDep_cmd_ext of phNxpNciHal_NfcDepSWPrio.cc, 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-10Android ID: A-139736125	4.4	More Details
CVE-2020-0152	In avb_vbmeta_image_verify of avb_vbmeta_image.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-10Android ID: A-145992159	4.4	More Details
CVE-2020-0154	In nci_proc_core_rsp of nci_hrcv.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141550919	4.4	More Details
CVE-2020-0158	In nfc_ncif_proc_t3t_polling_ntf of nfc_ncif.cc, 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-10Android ID: A-141547128	4.4	More Details
CVE-2020-0148	In btu_hcif_pin_code_request_evt, btu_hcif_link_key_request_evt, and btu_hcif_link_key_notification_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 via compromised device firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142638492	4.4	More Details
CVE-2020-13702	The Rolling Proximity Identifier used in the Apple/Google Exposure Notification API beta through 2020-05-29 enables attackers to circumvent Bluetooth Smart Privacy because there is a secondary temporary UID. An attacker with access to Beacon or IoT networks can seamlessly track individual device movement via a Bluetooth LE discovery mechanism.	4.3	More Details
CVE-2020-11840	Unauthorized information disclosure vulnerability in Micro Focus ArcSight Management Center product, Affecting versions 2.6.1, 2.7.x, 2.8.x, 2.9.x prior to 2.9.4. The vulnerabilities could be remotely exploited resulting unauthorized information disclosure.	4.3	More Details
CVE-2020-11841	Unauthorized information disclosure vulnerability in Micro Focus ArcSight Management Center product, Affecting versions 2.6.1, 2.7.x, 2.8.x, 2.9.x prior to 2.9.4. The vulnerabilities could be remotely exploited resulting unauthorized information disclosure.	4.3	More Details
CVE-2020-0199	In TimeCheck::TimeCheckThread::threadLoop of TimeCheck.cpp, there is a possible use-after-free due to a race condition. 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-142142406	4.1	More Details
CVE-2020-3930	GeoVision Door Access Control device family improperly stores and controls access to system logs, any users can read these logs.	4.0	More Details
CVE-2020-2023	Kata Containers doesn't restrict containers from accessing the guest's root filesystem device. Malicious containers can exploit this to gain code execution on the guest and masquerade as the kata-agent. This issue affects Kata Containers 1.11 versions earlier than 1.11.1; Kata Containers 1.10 versions earlier than 1.10.5; and Kata Containers 1.9 and earlier versions.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4051	In Dijit before versions 1.11.11, and greater than or equal to 1.12.0 and less than 1.12.9, and greater than or equal to 1.13.0 and less than 1.13.8, and greater than or equal to 1.14.0 and less than 1.14.7, and greater than or equal to 1.15.0 and less than 1.15.4, and greater than or equal to 1.16.0 and less than 1.16.3, there is a cross-site scripting vulnerability in the Editor's LinkDialog plugin. This has been fixed in 1.11.11, 1.12.9, 1.13.8, 1.14.7, 1.15.4, 1.16.3.	3.7	More Details
CVE-2020-4053	In Helm greater than or equal to 3.0.0 and less than 3.2.4, a path traversal attack is possible when installing Helm plugins from a tar archive over HTTP. It is possible for a malicious plugin author to inject a relative path into a plugin archive, and copy a file outside of the intended directory. This has been fixed in 3.2.4.	3.7	More Details
CVE-2020-4050	In affected versions of WordPress, misuse of the `set-screen-option` filter's return value allows arbitrary user meta fields to be saved. It does require an admin to install a plugin that would misuse the filter. Once installed, it can be leveraged by low privileged users. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).	3.5	More Details
CVE-2020-10732	A flaw was found in the Linux kernel's implementation of Userspace core dumps. This flaw allows an attacker with a local account to crash a trivial program and exfiltrate private kernel data.	3.3	More Details
CVE-2017-18869	A TOCTOU issue in the chownr package before 1.1.0 for Node.js 10.10 could allow a local attacker to trick it into descending into unintended directories via symlink attacks.	2.5	More Details
CVE-2020-4049	In affected versions of WordPress, when uploading themes, the name of the theme folder can be crafted in a way that could lead to JavaScript execution in /wp-admin on the themes page. This does require an admin to upload the theme, and is low severity self-XSS. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).	2.4	More Details
CVE-2020-14151	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2018-11813. Reason: This candidate is a duplicate of CVE-2018-11813. Notes: All CVE users should reference [ID] instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-6279	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-2020-10708	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-2019-5731	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-2019-5732	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-2019-5735	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