SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 23 September 2020

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-15188	SOY CMS 3.0.2.327 and earlier is affected by Unauthenticated Remote Code Execution (RCE). The allows remote attackers to execute any arbitrary code when the inquiry form feature is enabled by the service. The vulnerability is caused by unserializing the form without any restrictions. This was fixed in 3.0.2.328.	10.0	More Details
CVE-2020-14315	A memory corruption vulnerability is present in bspatch as shipped in Colin Percival's bsdiff tools version 4.3. Insufficient checks when handling external inputs allows an attacker to bypass the sanity checks in place and write out of a dynamically allocated buffer boundaries.	9.8	More Details
CVE-2020-11698	An issue was discovered in Titan SpamTitan 7.07. Improper input sanitization of the parameter community on the page snmp-x.php would allow a remote attacker to inject commands into the file snmpd.conf that would allow executing commands on the target server.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11857	An Authorization Bypass vulnerability on Micro Focus Operation Bridge Reporter, affecting version 10.40 and earlier. The vulnerability could allow remote attackers to access the OBR host as a non-admin user	9.8	More Details
CVE-2020-25787	An issue was discovered in Tiny Tiny RSS (aka tt-rss) before 2020-09-16. It does not validate all URLs before requesting them.	9.8	More Details
CVE-2020-8158	Prototype pollution vulnerability in the TypeORM package < 0.2.25 may allow attackers to add or modify Object properties leading to further denial of service or SQL injection attacks.	9.8	More Details
CVE-2020-0354	In Bluetooth, 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-11Android ID: A-143604331	9.8	More Details
CVE-2020-25756	A buffer overflow vulnerability exists in the mg_get_http_header function in Cesanta Mongoose 6.18 due to a lack of bounds checking. A crafted HTTP header can exploit this bug. NOTE: a committer has stated "this will not happen in practice.	9.8	More Details
CVE-2020-0333	In UrlQuerySanitizer, there is a possible improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-73822755	9.8	More Details
CVE-2020-25216	yWorks yEd Desktop before 3.20.1 allows code execution via an XSL Transformation when using an XML file in conjunction with a custom stylesheet.	9.8	More Details
CVE-2020-25215	yWorks yEd Desktop before 3.20.1 allows XXE attacks via an XML or GraphML document.	9.8	More Details
CVE-2020-25489	A heap overflow in Sqreen PyMiniRacer (aka Python Mini Racer) before 0.3.0 allows remote attackers to potentially exploit heap corruption.	9.8	More Details
CVE-2020-25412	com_line() in command.c in gnuplot 5.4 leads to an out-of-bounds-write from strncpy() that may lead to arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24753	A memory corruption vulnerability in Objective Open CBOR Run-time (oocborrt) in versions before 2020-08-12 could allow an attacker to execute code via crafted Concise Binary Object Representation (CBOR) input to the cbor2json decoder. An uncaught error while decoding CBOR Major Type 3 text strings leads to the use of an attacker-controllable uninitialized stack value. This can be used to modify memory, causing a crash or potentially exploitable heap corruption.	9.8	More Details
CVE-2020-0380	In allocExcessBits of bitalloc.c, there is a possible out of bounds write due to an incorrect 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-11 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-146398979	9.8	More Details
CVE-2020-0123	There is a possible out of bounds write due to an incorrect bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-149871374	9.8	More Details
CVE-2020-25614	xmlquery before 1.3.1 lacks a check for whether a LoadURL response is in the XML format, which allows attackers to cause a denial of service (SIGSEGV) at xmlquery.(*Node).InnerText or possibly have unspecified other impact.	9.8	More Details
CVE-2020-14509	Multiple memory corruption vulnerabilities exist in CodeMeter (All versions prior to 7.10) where the packet parser mechanism does not verify length fields. An attacker could send specially crafted packets to exploit these vulnerabilities.	9.8	More Details
CVE-2020-14517	Protocol encryption can be easily broken for CodeMeter (All versions prior to 6.90 are affected, including Version 6.90 or newer only if CodeMeter Runtime is running as server) and the server accepts external connections, which may allow an attacker to remotely communicate with the CodeMeter API.	9.8	More Details
CVE-2020-11856	Arbitrary code execution vulnerability on Micro Focus Operation Bridge Reporter, affecting version 10.40 and earlier. The vulnerability could allow remote attackers to execute arbitrary code on affected installations of OBR.	9.8	More Details
CVE-2020-0229	There is a possible out of bounds write due to an incorrect bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-156333725	9.8	More Details
CVE-2020-0278	There is a possible out of bounds write due to an incorrect bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-160812574	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0342	There is a possible out of bounds write due to an incorrect bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-160812576	9.8	More Details
CVE-2020-24377	A DNS rebinding vulnerability in the Freebox OS web interface in Freebox Server before 4.2.3.	9.6	More Details
CVE-2020-24376	A DNS rebinding vulnerability in the UPnP IGD implementations in Freebox v5 before 1.5.29 and Freebox Server before 4.2.3.	9.6	More Details
CVE-2020-15961	Insufficient policy validation in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	9.6	More Details
CVE-2020-15963	Insufficient policy enforcement in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	9.6	More Details
CVE-2020-6573	Use after free in video in Google Chrome on Android prior to 85.0.4183.102 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-24374	A DNS rebinding vulnerability in Freebox v5 before 1.5.29.	9.6	More Details
CVE-2020-8028	A Improper Access Control vulnerability in the configuration of salt of SUSE Linux Enterprise Module for SUSE Manager Server 4.1, SUSE Manager Proxy 4.0, SUSE Manager Retail Branch Server 4.0, SUSE Manager Server 3.2, SUSE Manager Server 4.0 allows local users to escalate to root on every system managed by SUSE manager. On the managing node itself code can be executed as user salt, potentially allowing for escalation to root there. This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.1 google-gson versions prior to 2.8.5-3.4.3, httpcomponents-client-4.5.6-3.4.2, httpcomponents-. SUSE Manager Proxy 4.0 release-notes-susemanager-proxy versions prior to 4.0.9-0.16.38.1. SUSE Manager Retail Branch Server 4.0 release-notes-susemanager-proxy versions prior to 4.0.9-0.16.38.1. SUSE Manager Server 3.2 salt-netapi-client versions prior to 0.16.0-4.14.1, spacewalk-. SUSE Manager Server 4.0 release-notes-susemanager versions prior to 4.0.9-3.54.1.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15181	The Alfresco Reset Password add-on before version 1.2.0 relies on untrusted inputs in a security decision. Intruders can get admin's access to the system using the vulnerability in the project. Impacts all servers where this add-on is installed. The problem is fixed in version 1.2.0	9.3	More Details
CVE-2020-13169	Stored XSS (Cross-Site Scripting) exists in the SolarWinds Orion Platform before before 2020.2.1 on multiple forms and pages. This vulnerability may lead to the Information Disclosure and Escalation of Privileges (takeover of administrator account).	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-6532	Use after free in SCTP in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-13948	While investigating a bug report on Apache Superset, it was determined that an authenticated user could craft requests via a number of templated text fields in the product that would allow arbitrary access to Python's `os` package in the web application process in versions < 0.37.1. It was thus possible for an authenticated user to list and access files, environment variables, and process information. Additionally it was possible to set environment variables for the current process, create and update files in folders writable by the web process, and execute arbitrary programs accessible by the web process. All other operations available to the `os` package in Python were also available, even if not explicitly enumerated in this CVE.	8.8	More Details
CVE-2020-4611	IBM Data Risk Manager (iDNA) 2.0.6 could allow an authenticated user to bypass security and execute actions reserved for admins. IBM X-Force ID: 184922.	8.8	More Details
CVE-2020-6545	Use after free in audio in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6146	An exploitable code execution vulnerability exists in the rendering functionality of Nitro Pro 13.13.2.242 and 13.16.2.300. When drawing the contents of a page and selecting the stroke color from an 'ICCBased' colorspace, the application will read a length from the file and use it as a loop sentinel when writing data into the member of an object. Due to the object member being a buffer of a static size allocated on the heap, this can result in a heap-based buffer overflow. A specially crafted document must be loaded by a victim in order to trigger this vulnerability.	8.8	More Details
CVE-2020-6544	Use after free in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-13259	A vulnerability in the web-based management interface of RAD SecFlow-1v os-image SF_0290_2.3.01.26 could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web UI on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. This could be exploited in conjunction with CVE-2020-13260.	8.8	More Details
CVE-2020-2276	Jenkins Selection tasks Plugin 1.0 and earlier executes a user-specified program on the Jenkins controller, allowing attackers with Job/Configure permission to execute an arbitrary system command on the Jenkins controller as the OS user that the Jenkins process is running as.	8.8	More Details
CVE-2020-25040	Sylabs Singularity through 3.6.2 has Insecure Permissions on temporary directories used in explicit and implicit container build operations, a different vulnerability than CVE-2020-25039.	8.8	More Details
CVE-2020-0264	In libstagefright, 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-11Android ID: A-116718596	8.8	More Details
CVE-2020-14306	An incorrect access control flaw was found in the operator, openshift-service-mesh/istio-rhel8-operator all versions through 1.1.3. This flaw allows an attacker with a basic level of access to the cluster to deploy a custom gateway/pod to any namespace, potentially gaining access to privileged service account tokens. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6543	Use after free in task scheduling in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6542	Use after free in ANGLE in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6541	Use after free in WebUSB in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-15960	Heap buffer overflow in storage in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	8.8	More Details
CVE-2020-6540	Buffer overflow in Skia in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6576	Use after free in offscreen canvas in Google Chrome prior to 85.0.4183.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-0321	In the mp3 extractor, there is a possible out of bounds write due to uninitialized data. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155171907	8.8	More Details
CVE-2020-15962	Insufficient policy validation in serial in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	8.8	More Details
CVE-2020-15964	Insufficient data validation in media in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6539	Use after free in CSS in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6537	Type confusion in V8 in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15965	Type confusion in V8 in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	8.8	More Details
CVE-2020-24373	A CSRF vulnerability in the UPnP MediaServer implementation in Freebox Server before 4.2.3.	8.8	More Details
CVE-2020-2268	A cross-site request forgery (CSRF) vulnerability in Jenkins MongoDB Plugin 1.3 and earlier allows attackers to gain access to some metadata of any arbitrary files on the Jenkins controller.	8.8	More Details
CVE-2020-7530	A CWE-285 Improper Authorization vulnerability exists in SCADAPack 7x Remote Connect (V3.6.3.574 and prior) which allows improper access to executable code folders.	8.8	More Details
CVE-2020-25751	The paGO Commerce plugin 2.5.9.0 for Joomla! allows SQL Injection via the administrator/index.php?option=com_pago&view=comments filter_published parameter.	8.8	More Details
CVE-2020-6556	Heap buffer overflow in SwiftShader in Google Chrome prior to 84.0.4147.135 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6553	Use after free in offline mode in Google Chrome on iOS prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6559	Use after free in presentation API in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6552	Use after free in Blink in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6551	Use after free in WebXR in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6550	Use after free in IndexedDB in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6549	Use after free in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-14026	CSV Injection (aka Excel Macro Injection or Formula Injection) exists in the Export Of Contacts feature in Ozeki NG SMS Gateway through 4.17.6 via a value that is mishandled in a CSV export.	8.8	More Details
CVE-2020-0245	In DecodeFrameCombinedMode of combined_decode.cpp, 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: AndroidVersions: Android-11 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-152496149	8.8	More Details
CVE-2020-14025	Ozeki NG SMS Gateway through 4.17.6 has multiple CSRF vulnerabilities. For example, an administrator, by following a link, can be tricked into making unwanted changes such as installing new modules or changing a password.	8.8	More Details
CVE-2020-8247	Citrix ADC and Citrix Gateway 13.0 before 13.0-64.35, Citrix ADC and NetScaler Gateway 12.1 before 12.1-58.15, Citrix ADC 12.1-FIPS before 12.1-55.187, Citrix ADC and NetScaler Gateway 12.0, Citrix ADC and NetScaler Gateway 11.1 before 11.1-65.12, Citrix SD-WAN WANOP 11.2 before 11.2.1a, Citrix SD-WAN WANOP 11.1 before 11.1.2a, Citrix SD-WAN WANOP 11.0 before 11.0.3f, Citrix SD-WAN WANOP 10.2 before 10.2.7b are vulnerable to escalation of privileges on the management interface.	8.8	More Details
CVE-2020-14022	Ozeki NG SMS Gateway 4.17.1 through 4.17.6 does not check the file type when bulk importing new contacts ("Import Contacts" functionality) from a file. It is possible to upload an executable or .bat file that can be executed with the help of a functionality (E.g. the "Application Starter" module) within the application.	8.8	More Details
CVE-2020-6548	Heap buffer overflow in Skia in Google Chrome prior to 84.0.4147.125 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-11699	An issue was discovered in Titan SpamTitan 7.07. Improper validation of the parameter fname on the page certs-x.php would allow an attacker to execute remote code on the target server. The user has to be authenticated before interacting with this page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11803	An issue was discovered in Titan SpamTitan 7.07. Improper sanitization of the parameter jaction when interacting with the page mailqueue.php could lead to PHP code evaluation server-side, because the user-provided input is passed directly to the php eval() function. The user has to be authenticated on the web platform before interacting with the page.	8.8	More Details
CVE-2020-2261	Jenkins Perfecto Plugin 1.17 and earlier executes a command on the Jenkins controller, allowing attackers with Job/Configure permission to run arbitrary commands on the Jenkins controller	8.8	More Details
CVE-2020-15776	An issue was discovered in Gradle Enterprise 2018.2 - 2020.2.4. The CSRF prevention token is stored in a request cookie that is not annotated as HttpOnly. An attacker with the ability to execute arbitrary code in a user's browser could impose an arbitrary value for this token, allowing them to perform cross-site request forgery.	8.8	More Details
CVE-2020-4621	IBM Data Risk Manager (iDNA) 2.0.6 could allow an authenticated user to escalate their privileges to administrator due to insufficient authorization checks. IBM X-Force ID: 184981.	8.8	More Details
CVE-2020-4620	IBM Data Risk Manager (iDNA) 2.0.6 could allow a remote authenticated attacker to upload arbitrary files, caused by the improper validation of file extensions. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to upload a malicious file, which could allow the attacker to execute arbitrary code on the vulnerable system. IBM X-Force ID: 184979.	8.8	More Details
CVE-2020-11804	An issue was discovered in Titan SpamTitan 7.07. Due to improper sanitization of the parameter quid, used in the page mailqueue.php, code injection can occur. The input for this parameter is provided directly by an authenticated user via an HTTP GET request.	8.8	More Details
CVE-2020-25728	The Reset Password add-on before 1.2.0 for Alfresco has a broken algorithm (involving an increment) that allows a malicious user to change any user's account password include the admin account.	8.8	More Details
CVE-2020-0303	In the Media extractor, there is a possible use after free due to improper locking. This could lead to remote code execution in the media extractor with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-148223229	8.8	More Details
CVE-2020-6554	Use after free in extensions in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially perform a sandbox escape via a crafted Chrome Extension.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15958	An issue was discovered in 1CRM System through 8.6.7. An insecure direct object reference to internally stored files allows a remote attacker to access various sensitive information via an unauthenticated request with a predictable URL.	8.6	More Details
CVE-2020-15183	SoyCMS 3.0.2 and earlier is affected by Reflected Cross-Site Scripting (XSS) which leads to Remote Code Execution (RCE) from a known vulnerability. This allows remote attackers to force the administrator to edit files once the adminsitrator loads a specially crafted webpage.	8.4	More Details
CVE-2020-25514	Sourcecodester Simple Library Management System 1.0 is affected by Incorrect Access Control via the Login Panel, http://<site>/lms/admin.php.	8.4	More Details
CVE-2020-15182	The SOY Inquiry component of SOY CMS is affected by Cross-site Request Forgery (CSRF) and Remote Code Execution (RCE). The vulnerability affects versions 2.0.0.3 and earlier of SOY Inquiry. This allows remote attackers to force the administrator to edit files once the administrator loads a specially crafted webpage. An administrator must be logged in for exploitation to be possible. This issue is fixed in SOY Inquiry version 2.0.0.4 and included in SOY CMS 3.0.2.328.	8.4	More Details
CVE-2020-6575	Race in Mojo in Google Chrome prior to 85.0.4183.102 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	8.3	More Details
CVE-2020-4409	IBM Maximo Asset Management 7.6.0 and 7.6.1 could allow a remote attacker to conduct phishing attacks, using a tabnabbing attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 179537.	8.2	More Details
CVE-2020-7734	All versions of package cabot are vulnerable to Cross-site Scripting (XSS) via the Endpoint column.	8.2	More Details
CVE-2020-25039	Sylabs Singularity 3.2.0 through 3.6.2 has Insecure Permissions on temporary directories used in fakeroot or user namespace container execution.	8.1	More Details
CVE-2020-25744	SaferVPN before 5.0.3.3 on Windows could allow low-privileged users to create or overwrite arbitrary files, which could cause a denial of service (DoS) condition, because a symlink from %LOCALAPPDATA%\SaferVPN\Log is followed.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4617	IBM Data Risk Manager (iDNA) 2.0.6 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 184930.	8.1	More Details
CVE-2020-24750	FasterXML jackson-databind 2.x before 2.9.10.6 mishandles the interaction between serialization gadgets and typing, related to com.pastdev.httpcomponents.configuration.JndiConfiguration.	8.1	More Details
CVE-2020-25788	An issue was discovered in Tiny Tiny RSS (aka tt-rss) before 2020-09-16. imgproxy in plugins/af_proxy_http/init.php mishandles $_REQUEST["url"] in an error message.	8.1	More Details
CVE-2020-0401	In setInstallerPackageName of PackageManagerService.java, there is a missing permission check. This could lead to local escalation of privilege and granting spurious permissions with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-150857253	7.8	More Details
CVE-2020-0430	In skb_headlen of /include/linux/skbuff.h, there is a possible out of bounds read due to memory corruption. 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-153881554	7.8	More Details
CVE-2020-3979	InstallBuilder for Qt Windows (versions prior to 20.7.0) installers look for plugins at a predictable location at initialization time, writable by non-admin users. While those plugins are not required, they are loaded if present, which could allow an attacker to plant a malicious library which could result in code execution with the security scope of the installer.	7.8	More Details
CVE-2020-0273	In hwservicemanager, there is a possible out of bounds write due to freeing a wild pointer. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155646800	7.8	More Details
CVE-2020-0298	In Bluetooth, there is a possible control over Bluetooth enabled state 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-11Android ID: A-145129266	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0262	In WiFi tethering, there is a possible attacker controlled intent due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156353008	7.8	More Details
CVE-2020-0089	In the audio server, there is a missing permission check. This could lead to local escalation of privilege regarding audio settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137015603	7.8	More Details
CVE-2020-8252	The implementation of realpath in libuv < 10.22.1, < 12.18.4, and < 14.9.0 used within Node.js incorrectly determined the buffer size which can result in a buffer overflow if the resolved path is longer than 256 bytes.	7.8	More Details
CVE-2020-0299	In Bluetooth, there is a possible spoofing of bluetooth device metadata due to a missing permission check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-145130119	7.8	More Details
CVE-2020-0405	In NetworkStackNotifier, there is a possible permissions bypass due to an unsafe implicit PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157475111	7.8	More Details
CVE-2020-0319	In NFC, 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 and a Firmware compromise needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137868765	7.8	More Details
CVE-2020-0387	In manifest files of the SmartSpace package, there is a possible tapjacking vector due to a missing permission check. This could lead to local escalation of privilege and account hijacking with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-156046804	7.8	More Details
CVE-2020-6546	Inappropriate implementation in installer in Google Chrome prior to 84.0.4147.125 allowed a local attacker to potentially elevate privilege via a crafted filesystem.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0394	In onCreate of BluetoothPairingDialog.java, there is a possible tapjacking vector due to an insecure default value. This could lead to local escalation of privilege and untrusted devices accessing contact lists with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-155648639	7.8	More Details
CVE-2020-11861	Unauthorized escalation of local privileges vulnerability on Micro Focus Operation Agent, affecting all versions prior to versions 12.11. The vulnerability could be exploited to escalate the local privileges and gain root access on the system.	7.8	More Details
CVE-2020-0306	In LLVM, there is a possible ineffective stack cookie placement due to stack frame double reservation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-139666480	7.8	More Details
CVE-2020-0432	In skb_to_mamac of networking.c, 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 not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-143560807	7.8	More Details
CVE-2020-0266	In factory reset protection, there is a possible FRP bypass 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-11Android ID: A-111086459	7.8	More Details
CVE-2020-0341	In DisplayManager, there is a possible permission bypass 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-11Android ID: A-144920149	7.8	More Details
CVE-2020-0345	In DocumentsUI, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-144286721	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0277	In NetworkPolicyManagerService, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege allowing a malicious app to modify the device's data plan with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-148627993	7.8	More Details
CVE-2020-0275	In MediaProvider, there is a possible way to access ContentResolver and MediaStore entries the app shouldn't have access to due to a permissions bypass. This could lead to local escalation of privilege, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150507736	7.8	More Details
CVE-2020-0346	In Mediaserver, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege if integer sanitization were not enabled (which it is by default), with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-147002762	7.8	More Details
CVE-2020-0267	In WindowManager, there is a possible launch of an unexpected app due to a confused deputy. This could lead to local escalation of privilege due to launching a malicious app instead of the one the user intended, with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-139128211	7.8	More Details
CVE-2020-0357	In SurfaceFlinger, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the graphics server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150225569	7.8	More Details
CVE-2020-0360	In Notification Access Confirmation, there is a possible permissions bypass due to uninformed consent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-145129456	7.8	More Details
CVE-2020-0433	In blk_mq_queue_tag_busy_iter of blk-mq-tag.c, there is a possible use after free due to improper locking. 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-151939299	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0366	In PackageInstaller, there is a possible permissions bypass due to a tapjacking vulnerability. This could lead to local escalation of privilege using an app set as the default Assist app with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-138443815	7.8	More Details
CVE-2020-0130	In screencap, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege in a system process with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-123230379	7.8	More Details
CVE-2020-0369	In libavb, 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 not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-130231426	7.8	More Details
CVE-2020-0374	In NFC, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156251602	7.8	More Details
CVE-2020-0375	In Telephony, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege and the setting of supported EUICC countries with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156253476	7.8	More Details
CVE-2020-0406	In libmpeg2dec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if another exploit allowed this to be triggered with different parameters, with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137794014	7.8	More Details
CVE-2020-0392	In getLayerDebugInfo of SurfaceFlinger.cpp, there is a possible code execution due to a double 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-9 Android-10 Android-11Android ID: A-150226608	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0434	In Pixel's use of the Catpipe library, 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-150730508	7.8	More Details
CVE-2020-25515	Sourcecodester Simple Library Management System 1.0 is affected by Insecure Permissions via Books > New Book , http://<site>/lms/index.php?page=books.	7.8	More Details
CVE-2020-0391	In applyPolicy of PackageManagerService.java, there is possible arbitrary command execution as System due to an unenforced protected-broadcast. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11Android ID: A-158570769	7.8	More Details
CVE-2020-6116	An arbitrary code execution vulnerability exists in the rendering functionality of Nitro Software, Inc.'s Nitro Pro 13.13.2.242. When drawing the contents of a page using colors from an indexed colorspace, the application can miscalculate the size of a buffer when allocating space for its colors. When using this allocated buffer, the application can write outside its bounds and cause memory corruption which can lead to code execution. A specially crafted document must be loaded by a victim in order to trigger this vulnerability.	7.8	More Details
CVE-2020-16202	WebAccess Node (All versions prior to 9.0.1) has incorrect permissions set for resources used by specific services, which may allow code execution with system privileges.	7.8	More Details
CVE-2020-7532	A CWE-502 Deserialization of Untrusted Data vulnerability exists in SCADAPack x70 Security Administrator (V1.2.0 and prior) which could allow arbitrary code execution when an attacker builds a custom .SDB file containing a malicious serialized buffer.	7.8	More Details
CVE-2020-7531	A CWE-284 Improper Access Control vulnerability exists in SCADAPack 7x Remote Connect (V3.6.3.574 and prior) which allows an attacker to place executables in a specific folder and run code whenever RemoteConnect is executed by the user.	7.8	More Details
CVE-2020-6574	Insufficient policy enforcement in installer in Google Chrome on OS X prior to 85.0.4183.102 allowed a local attacker to potentially achieve privilege escalation via a crafted binary.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7528	A CWE-502 Deserialization of Untrusted Data vulnerability exists in SCADAPack 7x Remote Connect (V3.6.3.574 and prior) which could allow arbitrary code execution when an attacker builds a custom .PRJ file containing a malicious serialized buffer.	7.8	More Details
CVE-2020-6112	An exploitable code execution vulnerability exists in the JPEG2000 Stripe Decoding functionality of Nitro Software, Inc.'s Nitro Pro 13.13.2.242 when decoding sub-samples. While initializing tiles with sub-sample data, the application can miscalculate a pointer for the stripes in the tile which allow for the decoder to write out of-bounds and cause memory corruption. This can result in code execution. A specially crafted image can be embedded inside a PDF and loaded by a victim in order to trigger this vulnerability.	7.8	More Details
CVE-2020-24889	A buffer overflow vulnerability in LibRaw version < 20.0 LibRaw::GetNormalizedModel in src/metadata/normalize_model.cpp may lead to context-dependent arbitrary code execution.	7.8	More Details
CVE-2020-25559	gnuplot 5.5 is affected by double free when executing print_set_output. This may result in context-dependent arbitrary code execution.	7.8	More Details
CVE-2020-6115	An exploitable vulnerability exists in the cross-reference table repairing functionality of Nitro Software, Inc.'s Nitro Pro 13.13.2.242. While searching for an object identifier in a malformed document that is missing from the cross-reference table, the application will save a reference to the object's cross-reference table entry inside a stack variable. If the referenced object identifier is not found, the application may resize the cross-reference table which can change the scope of its entry. Later when the application tries to reference cross-reference entry via the stack variable, the application will access memory belonging to the recently freed table causing a use-after-free condition. A specially crafted document can be delivered by an attacker and loaded by a victim in order to trigger this vulnerability.	7.8	More Details
CVE-2020-11855	An Authorization Bypass vulnerability on Micro Focus Operation Bridge Reporter, affecting version 10.40 and earlier. The vulnerability could allow local attackers on the OBR host to execute code with escalated privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6113	An exploitable vulnerability exists in the object stream parsing functionality of Nitro Software, Inc.'s Nitro Pro 13.13.2.242 when updating its cross-reference table. When processing an object stream from a PDF document, the application will perform a calculation in order to allocate memory for the list of indirect objects. Due to an error when calculating this size, an integer overflow may occur which can result in an undersized buffer being allocated. Later when initializing this buffer, the application can write outside its bounds which can cause a memory corruption that can lead to code execution. A specially crafted document can be delivered to a victim in order to trigger this vulnerability.	7.8	More Details
CVE-2020-25487	PHPGURUKUL Zoo Management System Using PHP and MySQL version 1.0 is affected by: SQL Injection via zms/animal-detail.php.	7.8	More Details
CVE-2020-0074	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-11 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-146204120	7.8	More Details
CVE-2020-0388	In createEmergencyLocationUserNotification of GnssVisibilityControl.java, there is a possible permissions bypass due to an empty mutable PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-156123285	7.8	More Details
CVE-2020-14382	A vulnerability was found in upstream release cryptsetup-2.2.0 where, there's a bug in LUKS2 format validation code, that is effectively invoked on every device/image presenting itself as LUKS2 container. The bug is in segments validation code in file 'lib/luks2/luks2_json_metadata.c' in function hdr_validate_segments(struct crypt_device *cd, json_object *hdr_jobj) where the code does not check for possible overflow on memory allocation used for intervals array (see statement "intervals = malloc(first_backup * sizeof(*intervals));"). Due to the bug, library can be *tricked* to expect such allocation was successful but for far less memory then originally expected. Later it may read data FROM image crafted by an attacker and actually write such data BEYOND allocated memory.	7.8	More Details
CVE-2020-6555	Out of bounds read in WebGL in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4581	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.12 could allow a remote attacker to cause a denial of service by sending a chunked transfer-encoding HTTP/2 request. IBM X-Force ID: 184441.	7.5	More Details
CVE-2020-4643	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information. IBM X-Force ID: 185590.	7.5	More Details
CVE-2020-25795	An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the Chunk implementation, insert_from can have a memory-safety issue upon a panic.	7.5	More Details
CVE-2020-4622	IBM Data Risk Manager (iDNA) 2.0.6 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: 184983.	7.5	More Details
CVE-2020-15775	An issue was discovered in Gradle Enterprise 2017.1 - 2020.2.4. The /usage page of Gradle Enterprise conveys high level build information such as project names and build counts over time. This page is incorrectly viewable anonymously.	7.5	More Details
CVE-2020-15771	An issue was discovered in Gradle Enterprise 2018.2 and Gradle Enterprise Build Cache Node 4.1. Cross-site transmission of cookie containing CSRF token allows remote attacker to bypass CSRF mitigation.	7.5	More Details
CVE-2020-8253	Improper authentication in Citrix XenMobile Server 10.12 before RP2, Citrix XenMobile Server 10.11 before RP4, Citrix XenMobile Server 10.10 before RP6 and Citrix XenMobile Server before 10.9 RP5 leads to the ability to access sensitive files.	7.5	More Details
CVE-2020-15768	An issue was discovered in Gradle Enterprise 2017.3 - 2020.2.4 and Gradle Enterprise Build Cache Node 1.0 - 9.2. Unrestricted HTTP header reflection in Gradle Enterprise allows remote attackers to obtain authentication cookies, if they are able to discover a separate XSS vulnerability. This potentially allows an attacker to impersonate another user. Gradle Enterprise affected application request paths:/info/headers, /cache-info/headers, /admin-info/headers, /distribution-broker-info/headers. Gradle Enterprise Build Cache Node affected application request paths:/cache-node-info/headers.	7.5	More Details
CVE-2020-4614	IBM Data Risk Manager (iDNA) 2.0.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt sensitive information. IBM X-Force ID: 184927.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25750	An issue was discovered in DotPlant2 before 2020-09-14. In class Pay2PayPayment in payment/Pay2PayPayment.php, there is an XXE vulnerability in the checkResult function. The user input ($_POST['xml']) is used for simplexml_load_string without sanitization. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.5	More Details
CVE-2020-4613	IBM Data Risk Manager (iDNA) 2.0.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 184925.	7.5	More Details
CVE-2020-25733	webTareas through 2.1 allows upload of the dangerous .exe and .shtml file types.	7.5	More Details
CVE-2020-25793	An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the Chunk implementation, the array size is not checked when constructed with From<InlineArray<A, T>>.	7.5	More Details
CVE-2020-7733	The package ua-parser-js before 0.7.22 are vulnerable to Regular Expression Denial of Service (ReDoS) via the regex for Redmi Phones and Mi Pad Tablets UA.	7.5	More Details
CVE-2020-4579	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.12 could allow a remote attacker to cause a denial of service by sending a specially crafted HTTP/2 request with invalid characters. IBM X-Force ID: 184438.	7.5	More Details
CVE-2020-8887	Telestream Tektronix Medius before 10.7.5 and Sentry before 10.7.5 have a SQL injection vulnerability allowing an unauthenticated attacker to dump database contents via the page parameter in a page=login request to index.php (aka the server login page).	7.5	More Details
CVE-2020-1748	A flaw was found in all supported versions before wildfly-elytron-1.6.8.Final-redhat-00001, where the WildFlySecurityManager checks were bypassed when using custom security managers, resulting in an improper authorization. This flaw leads to information exposure by unauthenticated access to secure resources.	7.5	More Details
CVE-2020-10758	A vulnerability was found in Keycloak before 11.0.1 where DoS attack is possible by sending twenty requests simultaneously to the specified keycloak server, all with a Content-Length header value that exceeds the actual byte count of the request body.	7.5	More Details
CVE-2020-25791	An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the Chunk implementation, the array size is not checked when constructed with unit().	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25796	An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the InlineArray implementation, an unaligned reference may be generated for a type that has a large alignment requirement.	7.5	More Details
CVE-2020-4580	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.12 could allow a remote attacker to cause a denial of service by sending a specially crafted a JSON request with invalid characters. IBM X-Force ID: 184439.	7.5	More Details
CVE-2020-8251	Node.js < 14.11.0 is vulnerable to HTTP denial of service (DoS) attacks based on delayed requests submission which can make the server unable to accept new connections.	7.5	More Details
CVE-2020-25792	An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the Chunk implementation, the array size is not checked when constructed with pair().	7.5	More Details
CVE-2020-25794	An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the Chunk implementation, clone can have a memory-safety issue upon a panic.	7.5	More Details
CVE-2020-5976	NVIDIA GeForce NOW, versions prior to 2.0.23 (Windows, macOS) and versions prior to 5.31 (Android, Shield TV), contains a vulnerability in the application software where the network test component transmits sensitive information insecurely, which may lead to information disclosure.	7.5	More Details
CVE-2020-5975	NVIDIA GeForce NOW, versions prior to 2.0.23 on Windows and macOS, contains a vulnerability in the desktop application software that includes sensitive information as part of a URL, which may lead to information disclosure.	7.5	More Details
CVE-2020-25766	An issue was discovered in MISP before 2.4.132. It can perform an unwanted action because of a POST operation on a form that is not linked to the login page.	7.5	More Details
CVE-2020-0286	In Bluetooth AVRCP, there is a possible leak of audio metadata due to residual data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150214479	7.5	More Details
CVE-2020-16233	An attacker could send a specially crafted packet that could have CodeMeter (All versions prior to 7.10) send back packets containing data from the heap.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14519	This vulnerability allows an attacker to use the internal WebSockets API for CodeMeter (All versions prior to 7.00 are affected, including Version 7.0 or newer with the affected WebSockets API still enabled. This is especially relevant for systems or devices where a web browser is used to access a web server) via a specifically crafted Java Script payload, which may allow alteration or creation of license files for when combined with CVE-2020-14515.	7.5	More Details
CVE-2020-14515	CodeMeter (All versions prior to 6.90 when using CmActLicense update files with CmActLicense Firm Code) has an issue in the license-file signature checking mechanism, which allows attackers to build arbitrary license files, including forging a valid license file as if it were a valid license file of an existing vendor. Only CmActLicense update files with CmActLicense Firm Code are affected.	7.5	More Details
CVE-2020-14513	CodeMeter (All versions prior to 6.81) and the software using it may crash while processing a specifically crafted license file due to unverified length fields.	7.5	More Details
CVE-2020-8225	A cleartext storage of sensitive information in Nextcloud Desktop Client 2.6.4 gave away information about used proxies and their authentication credentials.	7.5	More Details
CVE-2020-0300	In NFC, there is a possible out of bounds read due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-148736216	7.5	More Details
CVE-2020-8237	Prototype pollution in json-bigint npm package < 1.0.0 may lead to a denial-of-service (DoS) attack.	7.5	More Details
CVE-2020-14029	An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. The RSS To SMS module processes XML files in an unsafe manner. This opens the application to an XML External Entity attack that can be used to perform SSRF or read arbitrary local files.	7.5	More Details
CVE-2020-10718	A flaw was found in Wildfly before wildfly-embedded-13.0.0.Final, where the embedded managed process API has an exposed setting of the Thread Context Classloader (TCCL). This setting is exposed as a public method, which can bypass the security manager. The highest threat from this vulnerability is to confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0381	In Parse_wave of eas_mdls.c, there is a possible out of bounds write due to an integer overflow. This could lead to remote information disclosure in a highly constrained process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-150159669	7.5	More Details
CVE-2020-8246	Citrix ADC and Citrix Gateway 13.0 before 13.0-64.35, Citrix ADC and NetScaler Gateway 12.1 before 12.1-58.15, Citrix ADC 12.1-FIPS before 12.1-55.187, Citrix ADC and NetScaler Gateway 12.0, Citrix ADC and NetScaler Gateway 11.1 before 11.1-65.12, Citrix SD-WAN WANOP 11.2 before 11.2.1a, Citrix SD-WAN WANOP 11.1 before 11.1.2a, Citrix SD-WAN WANOP 11.0 before 11.0.3f, Citrix SD-WAN WANOP 10.2 before 10.2.7b are vulnerable to a denial of service attack originating from the management network.	7.5	More Details
CVE-2020-25727	The Reset Password add-on before 1.2.0 for Alfresco suffers from CMIS-SQL Injection, which allows a malicious user to inject a query within the email input field.	7.5	More Details
CVE-2020-8201	Node.js < 12.18.4 and < 14.11 can be exploited to perform HTTP desync attacks and deliver malicious payloads to unsuspecting users. The payloads can be crafted by an attacker to hijack user sessions, poison cookies, perform clickjacking, and a multitude of other attacks depending on the architecture of the underlying system. The attack was possible due to a bug in processing of carrier-return symbols in the HTTP header names.	7.4	More Details
CVE-2020-25490	Lack of cryptographic signature verification in the Sqreen PHP agent daemon before 1.16.0 makes it easier for remote attackers to inject rules for execution inside the virtual machine.	7.3	More Details
CVE-2020-10733	The Windows installer for PostgreSQL 9.5 - 12 invokes system-provided executables that do not have fully-qualified paths. Executables in the directory where the installer loads or the current working directory take precedence over the intended executables. An attacker having permission to add files into one of those directories can use this to execute arbitrary code with the installer's administrative rights.	7.3	More Details
CVE-2020-0271	In the Settings app, there is an insecure default value. This could lead to local escalation of privilege and tapjacking with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-144507081	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25790	Typesetter CMS 5.x through 5.1 allows admins to upload and execute arbitrary PHP code via a .php file inside a ZIP archive. NOTE: the vendor disputes the significance of this report because "admins are considered trustworthy"; however, the behavior "contradicts our security policy" and is being fixed for 5.2	7.2	More Details
CVE-2020-14031	An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. The outbox functionality of the TXT File module can be used to delete all/most files in a folder. Because the product usually runs as NT AUTHORITY\SYSTEM, the only files that will not be deleted are those currently being run by the system and/or files that have special security attributes (e.g., Windows Defender files).	7.2	More Details
CVE-2020-14028	An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. By leveraging a path traversal vulnerability in the Autoreply module's Script Name, an attacker may write to or overwrite arbitrary files, with arbitrary content, usually with NT AUTHORITY\SYSTEM privileges.	7.2	More Details
CVE-2020-24046	A sandbox escape issue was discovered in TitanHQ SpamTitan Gateway 7.07. It limits the admin user to a restricted shell, allowing execution of a small number of tools of the operating system. This restricted shell can be bypassed after changing the properties of the user admin in the operating system file /etc/passwd. This file cannot be accessed though the restricted shell, but it can be modified by abusing the Backup/Import Backup functionality of the web interface. An authenticated attacker would be able to obtain the file /var/tmp/admin.passwd after executing a Backup operation. This file can be manually modified to change the GUID of the user to 0 (root) and change the restricted shell to a normal shell /bin/sh. After the modification is done, the file can be recompressed to a .tar.bz file and imported again via the Import Backup functionality. The properties of the admin user will be overwritten and a root shell will be granted to the user upon the next successful login.	7.2	More Details
CVE-2020-24045	A sandbox escape issue was discovered in TitanHQ SpamTitan Gateway 7.07. It limits the admin user to a restricted shell, allowing execution of a small number of tools of the operating system. The restricted shell can be bypassed by presenting a fake vmware-tools ISO image to the guest virtual machine running SpamTitan Gateway. This ISO image should contain a valid Perl script at the vmware-freebsd-tools/vmware-tools-distrib/vmware-install.pl path. The fake ISO image will be mounted and the script wmware-install.pl will be executed with super-user privileges as soon as the hidden option to install VMware Tools is selected in the main menu of the restricted shell (option number 5). The contents of the script can be whatever the attacker wants, including a backdoor or similar.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14393	A buffer overflow was found in perl-DBI < 1.643 in DBI.xs. A local attacker who is able to supply a string longer than 300 characters could cause an out-of-bounds write, affecting the availability of the service or integrity of data.	7.1	More Details
CVE-2020-16247	Philips Clinical Collaboration Platform, Versions 12.2.1 and prior. The product exposes a resource to the wrong control sphere, providing unintended actors with inappropriate access to the resource.	7.1	More Details
CVE-2020-15774	An issue was discovered in Gradle Enterprise 2018.5 - 2020.2.4. An attacker with physical access to the browser of a user who has recently logged in to Gradle Enterprise and since closed their browser could reopen their browser to access Gradle Enterprise as that user.	6.8	More Details
CVE-2020-15189	SOY CMS 3.0.2 and earlier is affected by Remote Code Execution (RCE) using Unrestricted File Upload. Cross-Site Scripting(XSS) vulnerability that was used in CVE-2020-15183 can be used to increase impact by redirecting the administrator to access a specially crafted page. This vulnerability is caused by insecure configuration in elFinder. This is fixed in version 3.0.2.328.	6.8	More Details
CVE-2020-6781	Improper certificate validation for certain connections in the Bosch Smart Home System App for iOS prior to version 9.17.1 potentially allows to intercept video contents by performing a man-in-the-middle attack.	6.8	More Details
CVE-2020-0309	In the Bluetooth server, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System privileges and a Firmware compromise needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-147227320	6.7	More Details
CVE-2020-14386	A flaw was found in the Linux kernel before 5.9-rc4. Memory corruption can be exploited to gain root privileges from unprivileged processes. The highest threat from this vulnerability is to data confidentiality and integrity.	6.7	More Details
CVE-2020-0350	In NFC, 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 and a Firmware compromise needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-139424089	6.7	More Details
CVE-2020-0326	In NFC, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-146453119	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0347	In iptables, 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-11Android ID: A-136658008	6.7	More Details
CVE-2020-0356	In the Audio HAL, 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-11Android ID: A-143787559	6.7	More Details
CVE-2020-0335	In NFC, 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 and a Firmware compromise needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-122361504	6.7	More Details
CVE-2020-0330	In iorap, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege and code execution with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150331085	6.7	More Details
CVE-2020-3980	VMware Fusion (11.x) contains a privilege escalation vulnerability due to the way it allows configuring the system wide path. An attacker with normal user privileges may exploit this issue to trick an admin user into executing malicious code on the system where Fusion is installed.	6.7	More Details
CVE-2020-0334	In NFC, 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 and a Firmware compromise needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-147995915	6.7	More Details
CVE-2020-0336	In SurfaceFlinger, there is possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153467444	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0429	In l2tp_session_delete and related functions of l2tp_core.c, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-152735806	6.7	More Details
CVE-2020-0403	In the FPC TrustZone fingerprint App, there is a possible invalid command handler due to an exposed test feature. This could lead to local escalation of privilege in the TEE, with System execution privileges required. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-131252923	6.7	More Details
CVE-2020-0431	In kbd_keycode of keyboard.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-144161459	6.7	More Details
CVE-2020-24333	A vulnerability in Arista's CloudVision Portal (CVP) prior to 2020.2 allows users with "read-only" or greater access rights to the Configlet Management module to download files not intended for access, located on the CVP server, by accessing a specific API.	6.5	More Details
CVE-2020-15773	An issue was discovered in Gradle Enterprise before 2020.2.4. Because of unrestricted cross-origin requests to read-only data in the Export API, an attacker can access data as a user (for the duration of the browser session) after previously explicitly authenticating with the API.	6.5	More Details
CVE-2020-6565	Inappropriate implementation in Omnibox in Google Chrome on iOS prior to 85.0.4183.83 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2020-6567	Insufficient validation of untrusted input in command line handling in Google Chrome on Windows prior to 85.0.4183.83 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2020-25015	A specific router allows changing the Wi-Fi password remotely. Genexis Platinum 4410 V2-1.28, a compact router generally used at homes and offices was found to be vulnerable to Broken Access Control and CSRF which could be combined to remotely change the WIFI access point's password.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0353	In libmp4extractor, there is a 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-11Android ID: A-124777526	6.5	More Details
CVE-2020-3990	VMware Workstation (15.x) and Horizon Client for Windows (5.x before 5.4.4) contain an information disclosure vulnerability due to an integer overflow issue in Cortado ThinPrint component. A malicious actor with normal access to a virtual machine may be able to exploit this issue to leak memory from TPView process running on the system where Workstation or Horizon Client for Windows is installed. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon Client.	6.5	More Details
CVE-2020-6566	Insufficient policy enforcement in media in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2020-0279	In the AAC parser, 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-11Android ID: A-131430997	6.5	More Details
CVE-2020-0287	In libmkvextractor, there is a 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-11Android ID: A-141860394	6.5	More Details
CVE-2020-2254	Jenkins Blue Ocean Plugin 1.23.2 and earlier provides an undocumented feature flag that, when enabled, allows an attacker with Job/Configure or Job/Create permission to read arbitrary files on the Jenkins controller file system.	6.5	More Details
CVE-2020-0270	In tremolo, 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-11Android ID: A-145790628	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14177	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to impact the application's availability via a Regex-based Denial of Service (DoS) vulnerability in JQL version searching. The affected versions are before version 7.13.16; from version 7.14.0 before 8.5.7; from version 8.6.0 before 8.10.2; and from version 8.11.0 before 8.11.1.	6.5	More Details
CVE-2020-8200	Improper authentication in Citrix StoreFront Server < 1912.0.1000 allows an attacker who is authenticated on the same Microsoft Active Directory domain as a Citrix StoreFront server to read arbitrary files from that server.	6.5	More Details
CVE-2020-5421	In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.	6.5	More Details
CVE-2020-9084	Taurus-AN00B versions earlier than 10.1.0.156(C00E155R7P2) have a use-after-free (UAF) vulnerability. An authenticated, local attacker may perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege and compromise the service.	6.5	More Details
CVE-2020-6564	Inappropriate implementation in permissions in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to spoof the contents of a permission dialog via a crafted HTML page.	6.5	More Details
CVE-2020-6547	Incorrect security UI in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially obtain sensitive information via a crafted HTML page.	6.5	More Details
CVE-2020-16200	Philips Clinical Collaboration Platform, Versions 12.2.1 and prior. The software does not properly control the allocation and maintenance of a limited resource, thereby enabling an attacker to influence the amount of resources consumed, eventually leading to the exhaustion of available resources.	6.5	More Details
CVE-2020-11700	An issue was discovered in Titan SpamTitan 7.07. Improper sanitization of the parameter fname, used on the page certs-x.php, would allow an attacker to retrieve the contents of arbitrary files. The user has to be authenticated before interacting with this page.	6.5	More Details
CVE-2020-6563	Insufficient policy enforcement in intent handling in Google Chrome on Android prior to 85.0.4183.83 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24623	A potential security vulnerability has been identified in Hewlett Packard Enterprise Universal API Framework. The vulnerability could be remotely exploited to allow SQL injection in HPE Universal API Framework for VMware Esxi v2.5.2 and HPE Universal API Framework for Microsoft Hyper-V (VHD).	6.5	More Details
CVE-2020-6562	Insufficient policy enforcement in Blink in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2020-15839	Liferay Portal before 7.3.3, and Liferay DXP 7.1 before fix pack 18 and 7.2 before fix pack 6, does not restrict the size of a multipart/form-data POST action, which allows remote authenticated users to conduct denial-of-service attacks by uploading large files.	6.5	More Details
CVE-2020-6561	Inappropriate implementation in Content Security Policy in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2020-6560	Insufficient policy enforcement in autofill in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2020-6558	Insufficient policy enforcement in iOSWeb in Google Chrome on iOS prior to 85.0.4183.83 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2020-4619	IBM Data Risk Manager (iDNA) 2.0.6 stores user credentials in plain in clear text which can be read by an authenticated user. IBM X-Force ID: 184976.	6.5	More Details
CVE-2020-6568	Insufficient policy enforcement in intent handling in Google Chrome on Android prior to 85.0.4183.83 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2020-5629	UNIQLO App for Android versions 7.3.3 and earlier allows remote attackers to lead a user to access an arbitrary website via a malicious App created by the third party. As a result, if the access destination is a malicious website, the user may fall victim to the social engineering attack.	6.5	More Details
CVE-2020-0324	In libsonivox, 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-11Android ID: A-136660304	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0320	In libstagefright, there is a 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-11Android ID: A-129282427	6.5	More Details
CVE-2020-4590	IBM WebSphere Application Server Liberty 17.0.0.3 through 20.0.0.9 running oauth-2.0 or openidConnectServer-1.0 server features is vulnerable to a denial of service attack conducted by an authenticated client. IBM X-Force ID: 184650.	6.5	More Details
CVE-2020-0332	In libstagefright, there is a possible dead loop due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-124783982	6.5	More Details
CVE-2020-0370	In libAACdec, there is a possible out of bounds read due to 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-11Android ID: A-112051700	6.5	More Details
CVE-2020-2275	Jenkins Copy data to workspace Plugin 1.0 and earlier does not limit which directories can be copied from the Jenkins controller to job workspaces, allowing attackers with Job/Configure permission to read arbitrary files on the Jenkins controller.	6.5	More Details
CVE-2020-2277	Jenkins Storable Configs Plugin 1.0 and earlier allows users with Job/Read permission to read arbitrary files on the Jenkins controller.	6.5	More Details
CVE-2020-0364	In libDRCdec, 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-11Android ID: A-137282770	6.5	More Details
CVE-2020-0301	In libstagefright, there is a 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-11Android ID: A-124940460	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4612	IBM Data Risk Manager (iDNA) 2.0.6 could allow an authenticated user to obtain sensitive information using a specially crafted HTTP request. IBM X-Force ID: 184924.	6.5	More Details
CVE-2020-0363	In libmedia, there is a 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-11Android ID: A-132274514	6.5	More Details
CVE-2020-0362	In libstagefright, there is a 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-11Android ID: A-123237930	6.5	More Details
CVE-2020-6538	Inappropriate implementation in WebView in Google Chrome on Android prior to 84.0.4147.105 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2020-0361	In libDRCdec, 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-11Android ID: A-151927433	6.5	More Details
CVE-2020-2278	Jenkins Storable Configs Plugin 1.0 and earlier does not restrict the user-specified file name, allowing attackers with Job/Configure permission to replace any other '.xml' file on the Jenkins controller with a job config.xml file's content.	6.5	More Details
CVE-2020-0340	In libcodec2_soft_mp3dec, 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-11Android ID: A-144901522	6.5	More Details
CVE-2020-5628	UNIQLO App for Android versions 7.3.3 and earlier allows remote attackers to lead a user to access an arbitrary website via the vulnerable App. As a result, if the access destination is a malicious website, the user may fall victim to the social engineering attack.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16171	An issue was discovered in Acronis Cyber Backup before 12.5 Build 16342. Some API endpoints on port 9877 under /api/ams/ accept an additional custom Shard header. The value of this header is afterwards used in a separate web request issued by the application itself. This can be abused to conduct SSRF attacks against otherwise unreachable Acronis services that are bound to localhost such as the NotificationService on 127.0.0.1:30572.	6.5	More Details
CVE-2020-0351	In libstagefright, there is possible CPU 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-11Android ID: A-124777537	6.5	More Details
CVE-2020-0355	In libFraunhoferAAC, 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-11Android ID: A-141883493	6.5	More Details
CVE-2020-3977	VMware Horizon DaaS (7.x and 8.x before 8.0.1 Update 1) contains a broken authentication vulnerability due to a flaw in the way it handled the first factor authentication. Successful exploitation of this issue may allow an attacker to bypass two-factor authentication process. In order to exploit this issue, an attacker must have a legitimate account on Horizon DaaS.	6.5	More Details
CVE-2020-0428	In CamX code, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges required. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-123999783	6.4	More Details
CVE-2020-0358	In SurfaceFlinger, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150227563	6.4	More Details
CVE-2020-0268	In NFC, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-148294643	6.4	More Details
CVE-2020-6569	Integer overflow in WebUSB in Google Chrome prior to 85.0.4183.83 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16198	Philips Clinical Collaboration Platform, Versions 12.2.1 and prior. When an attacker claims to have a given identity, the software does not prove or insufficiently proves the claim is correct.	6.3	More Details
CVE-2020-13944	In Apache Airflow < 1.10.12, the "origin" parameter passed to some of the endpoints like '/trigger' was vulnerable to XSS exploit.	6.1	More Details
CVE-2020-13928	Apache Atlas before 2.1.0 contain a XSS vulnerability. While saving search or rendering elements values are not sanitized correctly and because of that it triggers the XSS vulnerability.	6.1	More Details
CVE-2020-15769	An issue was discovered in Gradle Enterprise 2020.2 - 2020.2.4. An XSS issue exists via the request URL.	6.1	More Details
CVE-2020-3988	VMware Workstation (15.x) and Horizon Client for Windows (5.x before 5.4.4) contain an out-of-bounds read vulnerability in Cortado ThinPrint component (JPEG2000 parser). A malicious actor with normal access to a virtual machine may be able to exploit these issues to create a partial denial-of-service condition or to leak memory from TPView process running on the system where Workstation or Horizon Client for Windows is installed.	6.1	More Details
CVE-2020-5606	Cross-site scripting vulnerability in WHR-G54S firmware 1.43 and earlier allows remote attackers to inject arbitrary script via a specially crafted page.	6.1	More Details
CVE-2020-25786	webinc/js/info.php on D-Link DIR-816L 2.06.B09_BETA and DIR-803 1.04.B02 devices allows XSS via the HTTP Referer header. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: this is typically not exploitable because of URL encoding (except in Internet Explorer) and because a web page cannot specify that a client should make an additional HTTP request with an arbitrary Referer header	6.1	More Details
CVE-2020-3986	VMware Workstation (15.x) and Horizon Client for Windows (5.x before 5.4.4) contain an out-of-bounds read vulnerability in Cortado ThinPrint component (EMF Parser). A malicious actor with normal access to a virtual machine may be able to exploit these issues to create a partial denial-of-service condition or to leak memory from TPView process running on the system where Workstation or Horizon Client for Windows is installed.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25735	webTareas through 2.1 allows XSS in clients/editclient.php, extensions/addextension.php, administration/add_announcement.php, administration/departments.php, administration/locations.php, expenses/claim_type.php, projects/editproject.php, and general/newnotifications.php.	6.1	More Details
CVE-2020-10748	A flaw was found in Keycloak's data filter, in version 10.0.1, where it allowed the processing of data URLs in some circumstances. This flaw allows an attacker to conduct cross-site scripting or further attacks.	6.1	More Details
CVE-2014-10402	An issue was discovered in the DBI module through 1.643 for Perl. DBD::File drivers can open files from folders other than those specifically passed via the f_dir attribute in the data source name (DSN). NOTE: this issue exists because of an incomplete fix for CVE-2014-10401.	6.1	More Details
CVE-2020-13260	A vulnerability in the web-based management interface of RAD SecFlow-1v through 2020-05-21 could allow an authenticated attacker to upload a JavaScript file, with a stored XSS payload, that will remain stored in the system as an OVPN file in Configuration-Services-Security-OpenVPN-Config or as the static key file in Configuration-Services-Security-OpenVPN-Static Keys. This payload will execute each time a user opens an affected web page. This could be exploited in conjunction with CVE-2020-13259.	6.1	More Details
CVE-2020-25729	ZoneMinder before 1.34.21 has XSS via the connkey parameter to download.php or export.php.	6.1	More Details
CVE-2020-25789	An issue was discovered in Tiny Tiny RSS (aka tt-rss) before 2020-09-16. The cached_url feature mishandles JavaScript inside an SVG document.	6.1	More Details
CVE-2020-9739	Adobe Media Encoder version 14.3.2 (and earlier versions) has an out-of-bounds read vulnerability that could be exploited to read past the end of an allocated buffer, possibly resulting in a crash or disclosure of sensitive information from other memory locations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	6.1	More Details
CVE-2020-9744	Adobe Media Encoder version 14.3.2 (and earlier versions) has an out-of-bounds read vulnerability that could be exploited to read past the end of an allocated buffer, possibly resulting in a crash or disclosure of sensitive information from other memory locations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9745	Adobe Media Encoder version 14.3.2 (and earlier versions) has an out-of-bounds read vulnerability that could be exploited to read past the end of an allocated buffer, possibly resulting in a crash or disclosure of sensitive information from other memory locations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	6.1	More Details
CVE-2020-14024	Ozeki NG SMS Gateway through 4.17.6 has multiple authenticated stored and/or reflected XSS vulnerabilities via the (1) Receiver or Recipient field in the Mailbox feature, (2) OZFORM_GROUPNAME field in the Group configuration of addresses, (3) listname field in the Defining address lists configuration, or (4) any GET Parameter in the /default URL of the application.	6.1	More Details
CVE-2020-4731	IBM Aspera Web Application 1.9.14 PL1 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: 188055.	6.1	More Details
CVE-2020-3987	VMware Workstation (15.x) and Horizon Client for Windows (5.x before 5.4.4) contain an out-of-bounds read vulnerability in Cortado ThinPrint component (EMR STRETCHDIBITS parser). A malicious actor with normal access to a virtual machine may be able to exploit these issues to create a partial denial-of-service condition or to leak memory from TPView process running on the system where Workstation or Horizon Client for Windows is installed.	6.1	More Details
CVE-2020-8245	Improper Input Validation on Citrix ADC and Citrix Gateway 13.0 before 13.0-64.35, Citrix ADC and NetScaler Gateway 12.1 before 12.1-58.15, Citrix ADC 12.1-FIPS before 12.1-55.187, Citrix ADC and NetScaler Gateway 12.0, Citrix ADC and NetScaler Gateway 11.1 before 11.1-65.12, Citrix SD-WAN WANOP 11.2 before 11.2.1a, Citrix SD-WAN WANOP 11.1 before 11.1.2a, Citrix SD-WAN WANOP 11.0 before 11.0.3f, Citrix SD-WAN WANOP 10.2 before 10.2.7b leads to an HTML Injection attack against the SSL VPN web portal.	6.1	More Details
CVE-2020-24619	In mainwindow.cpp in Shotcut before 20.09.13, the upgrade check misuses TLS because of setPeerVerifyMode(QSslSocket::VerifyNone). A man-in-the-middle attacker could offer a spoofed download resource.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7358	In AppSpider installer versions prior to 7.2.126, the AppSpider installer calls an executable which can be placed in the appropriate directory by an attacker with access to the local machine. This would prevent the installer from distinguishing between a valid executable called during an installation and any arbitrary code executable using the same file name.	5.8	More Details
CVE-2020-0379	In the Bluetooth service, there is a possible spoofing attack due to a logic error. This could lead to remote information disclosure of sensitive information with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-150156492	5.7	More Details
CVE-2020-7297	Privilege Escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows authenticated user interface user to access protected dashboard data via improper access control in the user interface.	5.7	More Details
CVE-2020-14390	A flaw was found in the Linux kernel in versions before 5.9-rc6. When changing screen size, an out-of-bounds memory write can occur leading to memory corruption or a denial of service. Due to the nature of the flaw, privilege escalation cannot be fully ruled out.	5.6	More Details
CVE-2020-7945	Local registry credentials were included directly in the CD4PE deployment definition, which could expose these credentials to users who should not have access to them. This is resolved in Continuous Delivery for Puppet Enterprise 4.0.1.	5.5	More Details
CVE-2020-0365	In netd, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137346580	5.5	More Details
CVE-2020-10768	A flaw was found in the Linux Kernel before 5.8-rc1 in the prctl() function, where it can be used to enable indirect branch speculation after it has been disabled. This call incorrectly reports it as being 'force disabled' when it is not and opens the system to Spectre v2 attacks. The highest threat from this vulnerability is to confidentiality.	5.5	More Details
CVE-2020-0331	In Settings, there is a possible permissions bypass. This could lead to local information disclosure of the device's IMEI with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-147309310	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0425	There is a possible way to view notifications even when the "Lockdown" feature is on. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-124000380	5.5	More Details
CVE-2020-0288	In PackageManager, there is a missing permission check. This could lead to local information disclosure across user boundaries with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153995991	5.5	More Details
CVE-2020-0289	In PackageManager, there is a missing permission check. This could lead to local information disclosure across users with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153996872	5.5	More Details
CVE-2020-0327	In core networking, there is a missing permission check. This could lead to local information disclosure of app network usage with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-129151407	5.5	More Details
CVE-2020-0293	In Java network APIs, there is possible access to sensitive network state due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation in Android versions: Android-11, Android ID: A-141455849	5.5	More Details
CVE-2020-0296	In ADB server and USB server, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153356209	5.5	More Details
CVE-2020-0297	In devicepolicy service, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155183624	5.5	More Details
CVE-2020-0308	In Window Manager, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153654357	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0312	In Battery Saver, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153879099	5.5	More Details
CVE-2020-0314	In AudioService, there are missing permission checks. This could lead to local information disclosure of audio configuration with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154934920	5.5	More Details
CVE-2020-0317	In UsageStatsManager, there is a possible access to protected data due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-119671929	5.5	More Details
CVE-2020-0323	In libavb, 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-11Android ID: A-146516087	5.5	More Details
CVE-2020-0329	In the OMX encoder, there is a possible out of bounds read due to invalid input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-63522940	5.5	More Details
CVE-2020-0337	In MediaProvider, there is a possible bypass of a permissions check due to a confused deputy. This could lead to local information disclosure, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-124329382	5.5	More Details
CVE-2020-0343	In NetworkStatsService, there is a possible access to protected data due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-119672472	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0344	In MediaProvider, there is a possible permissions bypass due to SQL injection. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-140729887	5.5	More Details
CVE-2020-0352	In MediaProvider, there is a possible permissions bypass due to SQL injection. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-132074310	5.5	More Details
CVE-2020-0359	In GLESRenderEngine, there is a possible out of bounds read due to a buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150303018	5.5	More Details
CVE-2020-0274	In the OMX parser, there is a possible information disclosure due to a returned raw pointer. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-120781925	5.5	More Details
CVE-2020-0125	In mediadrm, 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-11Android ID: A-137282168	5.5	More Details
CVE-2020-0427	In create_pinctrl of core.c, 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 kernelAndroid ID: A-140550171	5.5	More Details
CVE-2020-0385	In Parse_insh of eas_mdls.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote information disclosure in the media extractor with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.0 Android-8.1Android ID: A-150160041	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10781	A flaw was found in the Linux Kernel before 5.8-rc6 in the ZRAM kernel module, where a user with a local account and the ability to read the /sys/class/zram-control/hot_add file can create ZRAM device nodes in the /dev/ directory. This read allocates kernel memory and is not accounted for a user that triggers the creation of that ZRAM device. With this vulnerability, continually reading the device may consume a large amount of system memory and cause the Out-of-Memory (OOM) killer to activate and terminate random userspace processes, possibly making the system inoperable.	5.5	More Details
CVE-2020-14392	An untrusted pointer dereference flaw was found in Perl-DBI < 1.643. A local attacker who is able to manipulate calls to dbd_db_login6_sv() could cause memory corruption, affecting the service's availability.	5.5	More Details
CVE-2020-2274	Jenkins ElasTest Plugin 1.2.1 and earlier stores its server password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	5.5	More Details
CVE-2020-24890	libraw 20.0 has a null pointer dereference vulnerability in parse_tiff_ifd in src/metadata/tiff.cpp, which may result in context-dependent arbitrary code execution. Note: this vulnerability occurs only if you compile the software in a certain way	5.5	More Details
CVE-2020-7529	A CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Transversal') vulnerability exists in SCADAPack 7x Remote Connect (V3.6.3.574 and prior) which allows an attacker to place content in any unprotected folder on the target system using a crafted .RCZ file.	5.5	More Details
CVE-2020-0383	In Parse_ins of eas_mdls.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote information disclosure in the media extractor process with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-150160279	5.5	More Details
CVE-2020-0384	In Parse_art of eas_mdls.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote information disclosure in the media extractor with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-150159906	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0386	In onCreate of RequestPermissionActivity.java, there is a possible tapjacking vector due to an insecure default value. This could lead to local escalation of privilege allowing an attacker to set Bluetooth discoverability with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-155650356	5.5	More Details
CVE-2020-0404	In uvc_scan_chain_forward of uvc_driver.c, there is a possible linked list corruption due to an unusual root cause. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-111893654References: Upstream kernel	5.5	More Details
CVE-2020-0389	In createSaveNotification of RecordingService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-156959408	5.5	More Details
CVE-2020-0390	In the app zygote SE Policy, there is a possible 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-10 Android-11Android ID: A-157598026	5.5	More Details
CVE-2020-0393	In decrypt and decrypt_1_2 of CryptoPlugin.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-9 Android-10 Android-11Android ID: A-154123412	5.5	More Details
CVE-2020-0395	In showNotification of EmergencyCallbackModeService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-154124307	5.5	More Details
CVE-2020-0396	In various places in Telephony, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-155094269	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0397	In getNotificationBuilder of CarrierServiceStateTracker.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-155092443	5.5	More Details
CVE-2020-0399	In showLimitedSimFunctionWarningNotification of NotificationMgr.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android-11Android ID: A-153993591	5.5	More Details
CVE-2020-0372	In ActivityManager, there is a possible access to protected data due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-119673147	5.5	More Details
CVE-2020-0290	In PackageManager, there is a missing permission check. This could lead to local information disclosure across users with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153996866	5.5	More Details
CVE-2020-0426	In SyncManager, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154921790	5.5	More Details
CVE-2020-0295	In Telecom, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155650969	5.5	More Details
CVE-2020-0265	In Telephony, there are possible leaks of sensitive data due to missing permission checks. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150155839	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0269	In Android Auto Settings, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-151645626	5.5	More Details
CVE-2020-0276	In Telephony, there is a possible permission bypass due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156253586	5.5	More Details
CVE-2020-0284	In Telephony, there is a possible permission bypass due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156253784	5.5	More Details
CVE-2020-0285	In Telephony, there is a possible permission bypass due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156253479	5.5	More Details
CVE-2020-0294	In bindWallpaperComponentLocked of WallpaperManagerService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.0 Android-8.1 Android-9Android ID: A-154915372	5.5	More Details
CVE-2020-0302	In Settings, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-151646375	5.5	More Details
CVE-2020-0318	In the System UI, there is a possible system crash due to an uncaught exception. This could lead to local permanent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-33646131	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0304	In Settings, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-151645695	5.5	More Details
CVE-2020-0307	In Settings, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-151645867	5.5	More Details
CVE-2020-0310	In Settings, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153356468	5.5	More Details
CVE-2020-0311	In InputManagerService, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153878642	5.5	More Details
CVE-2020-0315	In Zen Mode, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155642026	5.5	More Details
CVE-2020-0316	In Telephony, there is a missing permission check. This could lead to local information disclosure of radio data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154934919	5.5	More Details
CVE-2020-0263	In the Accessibility service, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154913130	5.5	More Details
CVE-2020-0313	In NotificationManagerService, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154917989	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15770	An issue was discovered in Gradle Enterprise 2018.5. An attacker can potentially make repeated attempts to guess a local user's password, due to lack of lock-out after excessive failed logins.	5.5	More Details
CVE-2020-2269	Jenkins chosen-views-tabbar Plugin 1.2 and earlier does not escape view names in the dropdown to select views, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with the ability to configure views.	5.4	More Details
CVE-2020-2265	Jenkins Coverage/Complexity Scatter Plot Plugin 1.1.1 and earlier does not escape the method information in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide report files to the plugin's post-build step.	5.4	More Details
CVE-2020-4615	IBM Data Risk Manager (iDNA) 2.0.6 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: 184928.	5.4	More Details
CVE-2020-2256	Jenkins Pipeline Maven Integration Plugin 3.9.2 and earlier does not escape the upstream job's display name shown as part of a build cause, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2020-20406	A stored XSS vulnerability exists in the Custom Link Attributes control Affect function in Elementor Page Builder 2.9.2 and earlier versions. It is caused by inadequate filtering on the link custom attributes.	5.4	More Details
CVE-2020-2259	Jenkins computer-queue-plugin Plugin 1.5 and earlier does not escape the agent name in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Agent/Configure permission.	5.4	More Details
CVE-2020-2262	Jenkins Android Lint Plugin 2.6 and earlier does not escape the annotation message in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide report files to the plugin's post-build step.	5.4	More Details
CVE-2020-2263	Jenkins Radiator View Plugin 1.29 and earlier does not escape the full name of the jobs in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2020-2257	Jenkins Validating String Parameter Plugin 2.4 and earlier does not escape various user-controlled fields, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2264	Jenkins Custom Job Icon Plugin 0.2 and earlier does not escape the job descriptions in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2020-2270	Jenkins ClearCase Release Plugin 0.3 and earlier does not escape the composite baseline in badge tooltip, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2020-2266	Jenkins Description Column Plugin 1.3 and earlier does not escape the job description in the column tooltip, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2020-2271	Jenkins Locked Files Report Plugin 1.6 and earlier does not escape locked files' names in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2020-14027	An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. The database connection strings accept custom unsafe arguments, such as ENABLE_LOCAL_INFILE, that can be leveraged by attackers to enable MySQL Load Data Local (rogue MySQL server) attacks.	5.3	More Details
CVE-2020-25734	webTareas through 2.1 allows files/Default/ Directory Listing.	5.3	More Details
CVE-2020-14181	Affected versions of Atlassian Jira Server and Data Center allow an unauthenticated user to enumerate users via an Information Disclosure vulnerability in the /ViewUserHover.jspa endpoint. The affected versions are before version 7.13.6, from version 8.0.0 before 8.5.7, and from version 8.6.0 before 8.12.0.	5.3	More Details
CVE-2020-14179	Affected versions of Atlassian Jira Server and Data Center allow remote, unauthenticated attackers to view custom field names and custom SLA names via an Information Disclosure vulnerability in the /secure/QueryComponent!Default.jspa endpoint. The affected versions are before version 8.5.8, and from version 8.6.0 before 8.11.1.	5.3	More Details
CVE-2020-4616	IBM Data Risk Manager (iDNA) 2.0.6 could disclose sensitive username information to an attacker using a specially crafted HTTP request. IBM X-Force ID: 184929.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14338	A flaw was found in Wildfly's implementation of Xerces, specifically in the way the XMLSchemaValidator class in the JAXP component of Wildfly enforced the "use-grammar-pool-only" feature. This flaw allows a specially-crafted XML file to manipulate the validation process in certain cases. This issue is the same flaw as CVE-2020-14621, which affected OpenJDK, and uses a similar code. This flaw affects all Xerces JBoss versions before 2.12.0.SP3.	5.3	More Details
CVE-2020-25633	A flaw was found in RESTEasy client in all versions of RESTEasy up to 4.5.6.Final. It may allow client users to obtain the server's potentially sensitive information when the server got WebApplicationException from the RESTEasy client call. The highest threat from this vulnerability is to data confidentiality.	5.3	More Details
CVE-2020-23446	Verint Workforce Optimization suite 15.1 (15.1.0.37634) has Unauthenticated Information Disclosure via API	5.3	More Details
CVE-2020-1710	The issue appears to be that JBoss EAP 6.4.21 does not parse the field-name in accordance to RFC7230[1] as it returns a 200 instead of a 400.	5.3	More Details
CVE-2020-15767	An issue was discovered in Gradle Enterprise before 2020.2.5. The cookie used to convey the CSRF prevention token is not annotated with the “secure” attribute, which allows an attacker with the ability to MITM plain HTTP requests to obtain it, if the user mistakenly uses a HTTP instead of HTTPS address to access the server. This cookie value could then be used to perform CSRF.	5.3	More Details
CVE-2020-4708	IBM Security Trusteer Pinpoint Detect 11.6.5 could disclose some information due to using a wildcard in the Access-Control-Allow-Origin header. IBM X-Force ID: 187371.	5.3	More Details
CVE-2020-0338	In checkKeyIntent of AccountManagerService.java, there is a possible permission bypass. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-9Android ID: A-123700107	5.0	More Details
CVE-2020-1694	A flaw was found in all versions of Keycloak before 10.0.0, where the NodeJS adapter did not support the verify-token-audience. This flaw results in some users having access to sensitive information outside of their permissions.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4618	IBM Data Risk Manager (iDNA) 2.0.6 could allow a privileged user to cause a denial of service due to improper input validation. IBM X-Force ID: 184937.	4.9	More Details
CVE-2020-14023	Ozeki NG SMS Gateway through 4.17.6 allows SSRF via SMS WCF or RSS To SMS.	4.9	More Details
CVE-2020-0348	In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over NFC with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-139188582	4.9	More Details
CVE-2020-15772	An issue was discovered in Gradle Enterprise 2018.5 - 2020.2.4. When configuring Gradle Enterprise to integrate with a SAML identity provider, an XML metadata file can be uploaded by an administrator. The server side processing of this file dereferences XML External Entities (XXE), allowing a remote attacker with administrative access to perform server side request forgery.	4.9	More Details
CVE-2020-14021	An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. The ASP.net SMS module can be used to read and validate the source code of ASP files. By altering the path, it can be made to read any file on the Operating System, usually with NT AUTHORITY\SYSTEM privileges.	4.9	More Details
CVE-2020-2253	Jenkins Email Extension Plugin 2.75 and earlier does not perform hostname validation when connecting to the configured SMTP server.	4.8	More Details
CVE-2020-2252	Jenkins Mailer Plugin 1.32 and earlier does not perform hostname validation when connecting to the configured SMTP server.	4.8	More Details
CVE-2020-0373	In SoundTriggerHwService, there is a possible out of bounds read due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-146894086	4.7	More Details
CVE-2019-20919	An issue was discovered in the DBI module before 1.643 for Perl. The hv_fetch() documentation requires checking for NULL and the code does that. But, shortly thereafter, it calls SvOK(profile), causing a NULL pointer dereference.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0281	In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure. System execution privileges, a Firmware compromise, and User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137857778	4.5	More Details
CVE-2020-0282	In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure. System execution privileges, a Firmware compromise, and User interaction are needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-144506224	4.5	More Details
CVE-2020-0272	In libhwbinder, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges required. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-130166487	4.4	More Details
CVE-2020-0328	In the camera, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150156131	4.4	More Details
CVE-2020-0325	In NFC, there is 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-11Android ID: A-145079309	4.4	More Details
CVE-2020-0291	In Bluetooth, 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 and a compromised Firmware needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-146032016	4.4	More Details
CVE-2020-0349	In NFC, 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-11Android ID: A-139188779	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0407	In various functions in fscrypt_ice.c and related files in some implementations of f2fs encryption that use encryption hardware which only supports 32-bit IVs (Initialization Vectors), 64-bit IVs are used and later are truncated to 32 bits. This may cause IV reuse and thus weakened disk encryption. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-153450752References: N/A	4.4	More Details
CVE-2020-0292	In Bluetooth, 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 and a compromised Firmware needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-110107252	4.4	More Details
CVE-2020-0322	In apexd, 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-11Android ID: A-147002540	4.4	More Details
CVE-2020-2260	A missing permission check in Jenkins Perfecto Plugin 1.17 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified HTTP URL using attacker-specified credentials.	4.3	More Details
CVE-2020-2258	Jenkins Health Advisor by CloudBees Plugin 3.2.0 and earlier does not correctly perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to view that HTTP endpoint.	4.3	More Details
CVE-2020-2255	A missing permission check in Jenkins Blue Ocean Plugin 1.23.2 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	4.3	More Details
CVE-2020-7268	Path Traversal vulnerability in McAfee McAfee Email Gateway (MEG) prior to 7.6.406 allows remote attackers to traverse the file system to access files or directories that are outside of the restricted directory via external input to construct a path name that should be within a restricted directory.	4.3	More Details
CVE-2020-6570	Information leakage in WebRTC in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to obtain potentially sensitive information via a crafted WebRTC interaction.	4.3	More Details
CVE-2020-2267	A missing permission check in Jenkins MongoDB Plugin 1.3 and earlier allows attackers with Overall/Read permission to gain access to some metadata of any arbitrary files on the Jenkins controller.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15959	Insufficient policy enforcement in networking in Google Chrome prior to 85.0.4183.102 allowed an attacker who convinced the user to enable logging to obtain potentially sensitive information from process memory via social engineering.	4.3	More Details
CVE-2020-4315	IBM Business Automation Content Analyzer on Cloud 1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 177234.	4.3	More Details
CVE-2020-14180	Affected versions of Atlassian Jira Service Desk Server and Data Center allow remote attackers authenticated as a non-administrator user to view Project Request-Types and Descriptions, via an Information Disclosure vulnerability in the editform request-type-fields resource. The affected versions are before version 4.12.0.	4.3	More Details
CVE-2020-14506	Philips Clinical Collaboration Platform, Versions 12.2.1 and prior. The product receives input or data, but it does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly.	4.3	More Details
CVE-2020-2272	A missing permission check in Jenkins ElasTest Plugin 1.2.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials.	4.3	More Details
CVE-2020-14348	It was found in AMQ Online before 1.5.2 that injecting an invalid field to a user's AddressSpace configuration of the user namespace puts AMQ Online in an inconsistent state, where the AMQ Online components do not operate properly, such as the failure of provisioning and the failure of creating addresses, though this does not impact upon already existing messaging clients or brokers.	4.3	More Details
CVE-2020-10715	A content spoofing vulnerability was found in the openshift/console 3.11 and 4.x. This flaw allows an attacker to craft a URL and inject arbitrary text onto the error page that appears to be from the OpenShift instance. This attack could potentially convince a user that the inserted text is legitimate.	4.3	More Details
CVE-2020-6571	Insufficient data validation in Omnibox in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15966	Insufficient policy enforcement in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information via a crafted Chrome Extension.	4.3	More Details
CVE-2020-2273	A cross-site request forgery (CSRF) vulnerability in Jenkins ElasTest Plugin 1.2.1 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials.	4.3	More Details
CVE-2020-5605	Directory traversal vulnerability in WHR-G54S firmware 1.43 and earlier allows an attacker to access sensitive information such as setting values via unspecified vectors.	4.3	More Details
CVE-2020-15184	In Helm before versions 2.16.11 and 3.3.2 there is a bug in which the `alias` field on a `Chart.yaml` is not properly sanitized. This could lead to the injection of unwanted information into a chart. This issue has been patched in Helm 3.3.2 and 2.16.11. A possible workaround is to manually review the `dependencies` field of any untrusted chart, verifying that the `alias` field is either not used, or (if used) does not contain newlines or path characters.	3.7	More Details
CVE-2020-14525	Philips Clinical Collaboration Platform, Versions 12.2.1 and prior. The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output used as a webpage that is served to other users.	3.5	More Details
CVE-2020-15186	In Helm before versions 2.16.11 and 3.3.2 plugin names are not sanitized properly. As a result, a malicious plugin author could use characters in a plugin name that would result in unexpected behavior, such as duplicating the name of another plugin or spoofing the output to `helm --help`. This issue has been patched in Helm 3.3.2. A possible workaround is to not install untrusted Helm plugins. Examine the `name` field in the `plugin.yaml` file for a plugin, looking for characters outside of the [a-zA-Z0-9._-] range.	3.4	More Details
CVE-2020-3989	VMware Workstation (15.x) and Horizon Client for Windows (5.x before 5.4.4) contain a denial of service vulnerability due to an out-of-bounds write issue in Cortado ThinPrint component. A malicious actor with normal access to a virtual machine may be able to exploit this issue to create a partial denial-of-service condition on the system where Workstation or Horizon Client for Windows is installed. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon Client.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15187	In Helm before versions 2.16.11 and 3.3.2, a Helm plugin can contain duplicates of the same entry, with the last one always used. If a plugin is compromised, this lowers the level of access that an attacker needs to modify a plugin's install hooks, causing a local execution attack. To perform this attack, an attacker must have write access to the git repository or plugin archive (.tgz) while being downloaded (which can occur during a MITM attack on a non-SSL connection). This issue has been patched in Helm 2.16.11 and Helm 3.3.2. As a possible workaround make sure to install plugins using a secure connection protocol like SSL.	3.0	More Details
CVE-2020-16230	All version of Ewon Flexy and Cosy prior to 14.1 use wildcards such as (*) under which domains can request resources. An attacker with local access and high privileges could inject scripts into the Cross-origin Resource Sharing (CORS) configuration that could abuse this vulnerability, allowing the attacker to retrieve limited confidential information through sniffing.	2.3	More Details
CVE-2020-0382	In RunInternal of dumpstate.cpp, there is a possible user consent bypass due to an uncaught exception. This could lead to local information disclosure of bug report data with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-152944488	2.3	More Details
CVE-2020-15185	In Helm before versions 2.16.11 and 3.3.2, a Helm repository can contain duplicates of the same chart, with the last one always used. If a repository is compromised, this lowers the level of access that an attacker needs to inject a bad chart into a repository. To perform this attack, an attacker must have write access to the index file (which can occur during a MITM attack on a non-SSL connection). This issue has been patched in Helm 3.3.2 and 2.16.11. A possible workaround is to manually review the index file in the Helm repository cache before installing software.	2.2	More Details
CVE-2020-0435	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2018-14615. Reason: This candidate is a duplicate of CVE-2018-14615. Notes: All CVE users should reference CVE-2018-14615 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-24891	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