SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 12 August 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-2020-7356	CAYIN xPost suffers from an unauthenticated SQL Injection vulnerability. Input passed via the GET parameter 'wayfinder_seqid' in wayfinder_meeting_input.jsp is not properly sanitized before being returned to the user or used in SQL queries. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code and execute SYSTEM commands.	10.0	More Details
CVE-2020-13151	Aerospike Community Edition 4.9.0.5 allows for unauthenticated submission and execution of user-defined functions (UDFs), written in Lua, as part of a database query. It attempts to restrict code execution by disabling os.execute() calls, but this is insufficient. Anyone with network access can use a crafted UDF to execute arbitrary OS commands on all nodes of the cluster at the permission level of the user running the Aerospike service.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13921	**Resolved** Only when using H2/MySQL/TiDB as Apache SkyWalking storage, there is a SQL injection vulnerability in the wildcard query cases.	9.8	More Details
CVE-2020-0253	There is a possible memory corruption due to a use after free.Product: AndroidVersions: Android SoCAndroid ID: A-152647365	9.8	More Details
CVE-2020-0252	There is a possible memory corruption due to a use after free.Product: AndroidVersions: Android SoCAndroid ID: A-152236803	9.8	More Details
CVE-2020-17466	Turcom TRCwifiZone through 2020-08-10 allows authentication bypass by visiting manage/control.php and ignoring 302 Redirect responses.	9.8	More Details
CVE-2020-17368	Firejail through 0.9.62 mishandles shell metacharacters during use of the --output or --output-stderr option, which may lead to command injection.	9.8	More Details
CVE-2020-11552	An elevation of privilege vulnerability exists in ManageEngine ADSelfService Plus before build 6003 because it does not properly enforce user privileges associated with a Certificate dialog. This vulnerability could allow an unauthenticated attacker to escalate privileges on a Windows host. An attacker does not require any privilege on the target system in order to exploit this vulnerability. One option is the self-service option on the Windows login screen. Upon selecting this option, the thick-client software is launched, which connects to a remote ADSelfService Plus server to facilitate self-service operations. An unauthenticated attacker having physical access to the host could trigger a security alert by supplying a self-signed SSL certificate to the client. The View Certificate option from the security alert allows an attacker to export a displayed certificate to a file. This can further cascade to a dialog that can open Explorer as SYSTEM. By navigating from Explorer to \windows\system32, cmd.exe can be launched as a SYSTEM.	9.8	More Details
CVE-2020-17479	jpv (aka Json Pattern Validator) before 2.2.2 does not properly validate input, as demonstrated by a corrupted array.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9529	Firmware developed by Shenzhen Hichip Vision Technology (V6 through V20), as used by many different vendors in millions of Internet of Things devices, suffers from a privilege escalation vulnerability that allows attackers on the local network to reset the device's administrator password. This affects products marketed under the following brand names: Accfly, Alptop, Anlink, Besdersec, BOAVISION, COOAU, CPVAN, Ctronics, D3D Security, Dericam, Elex System, Elite Security, ENSTER, ePGes, Escam, FLOUREON, GENBOLT, Hongjingtian (HJT), ICAMI, Iegeek, Jecurity, Jennov, KKMoon, LEFTEK, Loosafe, Luowice, Nesuniq, Nettoly, ProElite, QZT, Royallite, SDETER, SV3C, SY2L, Tenvis, ThinkValue, TOMLOV, TPTEK, WGCC, and ZILINK.	9.8	More Details
CVE-2020-9527	Firmware developed by Shenzhen Hichip Vision Technology (V6 through V20, after 2018-08-09 through 2020), as used by many different vendors in millions of Internet of Things devices, suffers from buffer overflow vulnerability that allows unauthenticated remote attackers to execute arbitrary code via the peer-to-peer (P2P) service. This affects products marketed under the following brand names: Accfly, Alptop, Anlink, Besdersec, BOAVISION, COOAU, CPVAN, Ctronics, D3D Security, Dericam, Elex System, Elite Security, ENSTER, ePGes, Escam, FLOUREON, GENBOLT, Hongjingtian (HJT), ICAMI, Iegeek, Jecurity, Jennov, KKMoon, LEFTEK, Loosafe, Luowice, Nesuniq, Nettoly, ProElite, QZT, Royallite, SDETER, SV3C, SY2L, Tenvis, ThinkValue, TOMLOV, TPTEK, WGCC, and ZILINK.	9.8	More Details
CVE-2020-16169	Authentication Bypass Using an Alternate Path or Channel in temi Robox OS prior to120, temi Android app up to 1.3.7931 allows remote attackers to gain elevated privileges on the temi and have it automatically answer the attacker's calls, granting audio, video, and motor control via unspecified vectors.	9.8	More Details
CVE-2020-11984	Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE	9.8	More Details
CVE-2020-13793	Unsafe storage of AD credentials in Ivanti DSM netinst 5.1 due to a static, hard-coded encryption key.	9.8	More Details
CVE-2020-12441	Denial-of-Service (DoS) in Ivanti Service Manager HEAT Remote Control 7.4 due to a buffer overflow in the protocol parser of the ‘HEATRemoteService’ agent. The DoS can be triggered by sending a specially crafted network packet.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5609	Directory traversal vulnerability in CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to create or overwrite arbitrary files and run arbitrary commands via unspecified vectors.	9.8	More Details
CVE-2020-5608	CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to bypass authentication and send altered communication packets via unspecified vectors.	9.8	More Details
CVE-2020-17353	scm/define-stencil-commands.scm in LilyPond through 2.20.0, and 2.21.x through 2.21.4, when -dsafe is used, lacks restrictions on embedded-ps and embedded-svg, as demonstrated by including dangerous PostScript code.	9.8	More Details
CVE-2020-13292	In GitLab before 13.0.12, 13.1.6 and 13.2.3, it is possible to bypass E-mail verification which is required for OAuth Flow.	9.6	More Details
CVE-2020-7361	The EasyCorp ZenTao Pro application suffers from an OS command injection vulnerability in its '/pro/repo-create.html' component. After authenticating to the ZenTao dashboard, attackers may construct and send arbitrary OS commands via the POST parameter 'path', and those commands will run in an elevated SYSTEM context on the underlying Windows operating system.	9.6	More Details
CVE-2020-7357	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5.	9.6	More Details
CVE-2020-16167	Missing Authentication for Critical Function in temi Robox OS prior to 120, temi Android app up to 1.3.7931 allows remote attackers to receive and answer calls intended for another temi user. Answering the call this way grants motor control of the temi in addition to audio/video via unspecified vectors.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14325	Red Hat CloudForms before 5.11.7.0 was vulnerable to the User Impersonation authorization flaw which allows malicious attacker to create existent and non-existent role-based access control user, with groups and roles. With a selected group of EvmGroup-super_administrator, an attacker can perform any API request as a super administrator.	9.1	More Details
CVE-2020-14324	A high severity vulnerability was found in all active versions of Red Hat CloudForms before 5.11.7.0. The out of band OS command injection vulnerability can be exploited by authenticated attacker while setuping conversion host through Infrastructure Migration Solution. This flaw allows attacker to execute arbitrary commands on CloudForms server.	9.1	More Details
CVE-2020-0260	There is a possible out of bounds read due to an incorrect bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-152225183	9.1	More Details
CVE-2020-13376	SecurEnvoy SecurMail 9.3.503 allows attackers to upload executable files and achieve OS command execution via a crafted SecurEnvoyReply cookie.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-13124	SABnzbd 2.3.9 and 3.0.0Alpha2 has a command injection vulnerability in the web configuration interface that permits an authenticated user to execute arbitrary Python commands on the underlying operating system.	8.8	More Details
CVE-2020-15062	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic.	8.8	More Details
CVE-2020-15817	In JetBrains YouTrack before 2020.1.1331, an external user could execute commands against arbitrary issues.	8.8	More Details
CVE-2020-9079	FusionSphere OpenStack 8.0.0 have a protection mechanism failure vulnerability. The product incorrectly uses a protection mechanism. An attacker has to find a way to exploit the vulnerability to conduct directed attacks against the affected product.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16277	An SQL injection vulnerability in the Analytics component of SAINT Security Suite 8.0 through 9.8.20 allows a remote, authenticated attacker to gain unauthorized access to the database.	8.8	More Details
CVE-2020-16276	An SQL injection vulnerability in the Assets component of SAINT Security Suite 8.0 through 9.8.20 allows a remote, authenticated attacker to gain unauthorized access to the database.	8.8	More Details
CVE-2020-15058	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic.	8.8	More Details
CVE-2020-11852	DKIM key management page vulnerability on Micro Focus Secure Messaging Gateway (SMG). Affecting all SMG Appliance running releases prior to July 2020. The vulnerability could allow a logged in user with rights to generate DKIM key information to inject system commands into the call to the DKIM system command.	8.8	More Details
CVE-2020-15824	In JetBrains Kotlin from 1.4-M1 to 1.4-RC (as Kotlin 1.3.7x is not affected by the issue. Fixed version is 1.4.0) there is a script-cache privilege escalation vulnerability due to kotlin-main-kts cached scripts in the system temp directory, which is shared by all users by default.	8.8	More Details
CVE-2020-0240	In NewFixedDoubleArray of factory.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-150706594	8.8	More Details
CVE-2020-15825	In JetBrains TeamCity before 2020.1, users with the Modify Group permission can elevate other users' privileges.	8.8	More Details
CVE-2020-15139	In MyBB before version 1.8.24, the custom MyCode (BBCode) for the visual editor doesn't escape input properly when rendering HTML, resulting in a DOM-based XSS vulnerability. The weakness can be exploited by pointing a victim to a page where the visual editor is active (e.g. as a post or Private Message) and operates on a maliciously crafted MyCode message. This may occur on pages where message content is pre-filled using a GET/POST parameter, or on reply pages where a previously saved malicious message is quoted. After upgrading MyBB to 1.8.24, make sure to update the version attribute in the `codebuttons` template for non-default themes to serve the latest version of the patched `jscripts/bbcodes_sceditor.js` file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13365	Certain Zyxel products have a locally accessible binary that allows a non-root user to generate a password for an undocumented user account that can be used for a TELNET session as root. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0.	8.8	More Details
CVE-2020-13364	A backdoor in certain Zyxel products allows remote TELNET access via a CGI script. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0.	8.8	More Details
CVE-2020-7810	hslogin2.dll ActiveX Control in Groupware contains a vulnerability that could allow remote files to be downloaded and executed by setting the arguments to the activex method. This is due to a lack of integrity verification of the policy files referenced in the update process, and a remote attacker could induce a user to crafted web page, causing damage such as malicious code infection.	8.8	More Details
CVE-2020-15063	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter.	8.8	More Details
CVE-2020-15480	An issue was discovered in PassMark BurnInTest through 9.1, OSForensics through 7.1, and PerformanceTest through 10. The kernel driver exposes IOCTL functionality that allows low-privilege users to read and write to arbitrary Model Specific Registers (MSRs). This could lead to arbitrary Ring-0 code execution and escalation of privileges. This affects DirectIo32.sys and DirectIo64.sys.	8.8	More Details
CVE-2020-15479	An issue was discovered in PassMark BurnInTest through 9.1, OSForensics through 7.1, and PerformanceTest through 10. The driver's IOCTL request handler attempts to copy the input buffer onto the stack without checking its size and can cause a buffer overflow. This could lead to arbitrary Ring-0 code execution and escalation of privileges. This affects DirectIo32.sys and DirectIo64.sys.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15055	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter.	8.8	More Details
CVE-2020-13404	The ATOS/Sips (aka Atos-Magento) community module 3.0.0 to 3.0.5 for Magento allows command injection.	8.8	More Details
CVE-2020-15656	JIT optimizations involving the Javascript arguments object could confuse later optimizations. This risk was already mitigated by various precautions in the code, resulting in this bug rated at only moderate severity. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.	8.8	More Details
CVE-2020-15059	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter.	8.8	More Details
CVE-2020-15054	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic.	8.8	More Details
CVE-2020-15659	Mozilla developers and community members reported memory safety bugs present in Firefox 78 and Firefox ESR 78.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1.	8.8	More Details
CVE-2020-6145	An SQL injection vulnerability exists in the frappe.desk.reportview.get functionality of ERPNext 11.1.38. A specially crafted HTTP request can cause an SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-17352	Two OS command injection vulnerabilities in the User Portal of Sophos XG Firewall through 2020-08-05 potentially allow an authenticated attacker to remotely execute arbitrary code.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8026	A Incorrect Default Permissions vulnerability in the packaging of inn in openSUSE Leap 15.2, openSUSE Tumbleweed, openSUSE Leap 15.1 allows local attackers with control of the new user to escalate their privileges to root. This issue affects: openSUSE Leap 15.2 inn version 2.6.2-lp152.1.26 and prior versions. openSUSE Tumbleweed inn version 2.6.2-4.2 and prior versions. openSUSE Leap 15.1 inn version 2.5.4-lp151.3.3.1 and prior versions.	8.4	More Details
CVE-2020-7352	The GalaxyClientService component of GOG Galaxy runs with elevated SYSTEM privileges in a Windows environment. Due to the software shipping with embedded, static RSA private key, an attacker with this key material and local user permissions can effectively send any operating system command to the service for execution in this elevated context. The service listens for such commands on a locally-bound network port, localhost:9978. A Metasploit module has been published which exploits this vulnerability. This issue affects the 2.0.x branch of the software (2.0.12 and earlier) as well as the 1.2.x branch (1.2.64 and earlier). A fix was issued for the 2.0.x branch of the affected software.	8.4	More Details
CVE-2020-10783	Red Hat CloudForms 4.7 and 5 is affected by a role-based privilege escalation flaw. An attacker with EVM-Operator group can perform actions restricted only to EVM-Super-administrator group, leads to, exporting or importing administrator files.	8.3	More Details
CVE-2020-4481	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 7.0.3.0, and 7.0.4.0 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 or consume memory resources. IBM X-Force ID: 181848.	8.2	More Details
CVE-2020-16253	The PgHero gem through 2.6.0 for Ruby allows CSRF.	8.1	More Details
CVE-2020-4486	IBM QRadar 7.2.0 thorugh 7.2.9 could allow an authenticated user to overwrite or delete arbitrary files due to a flaw after WinCollect installation. IBM X-Force ID: 181861.	8.1	More Details
CVE-2020-9525	CS2 Network P2P through 3.x, as used in millions of Internet of Things devices, suffers from an authentication flaw that allows remote attackers to perform a man-in-the-middle attack, as demonstrated by eavesdropping on user video/audio streams, capturing credentials, and compromising devices.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17367	Firejail through 0.9.62 does not honor the -- end-of-options indicator after the --output option, which may lead to command injection.	7.8	More Details
CVE-2020-16225	Delta Electronics TPEditor Versions 1.97 and prior. A write-what-where condition may be exploited by processing a specially crafted project file. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application.	7.8	More Details
CVE-2020-13177	The support bundler in Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows versions prior to 20.04.1 and 20.07.0 does not use hard coded paths for certain Windows binaries, which allows an attacker to gain elevated privileges via execution of a malicious binary placed in the system path.	7.8	More Details
CVE-2020-16227	Delta Electronics TPEditor Versions 1.97 and prior. An improper input validation may be exploited by processing a specially crafted project file not validated when the data is entered by a user. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application.	7.8	More Details
CVE-2020-14979	The WinRing0.sys and WinRing0x64.sys drivers 1.2.0 in EVGA Precision X1 through 1.0.6 allow local users, including low integrity processes, to read and write to arbitrary memory locations. This allows any user to gain NT AUTHORITY\SYSTEM privileges by mapping \Device\PhysicalMemory into the calling process.	7.8	More Details
CVE-2020-17448	Telegram Desktop through 2.1.13 allows a spoofed file type to bypass the Dangerous File Type Execution protection mechanism, as demonstrated by use of the chat window with a filename that lacks an extension.	7.8	More Details
CVE-2020-16221	Delta Electronics TPEditor Versions 1.97 and prior. A stack-based buffer overflow may be exploited by processing a specially crafted project file. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application.	7.8	More Details
CVE-2020-16223	Delta Electronics TPEditor Versions 1.97 and prior. A heap-based buffer overflow may be exploited by processing a specially crafted project file. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8224	A code injection in Nextcloud Desktop Client 2.6.4 allowed to load arbitrary code when placing a malicious OpenSSL config into a fixed directory.	7.8	More Details
CVE-2020-16219	Delta Electronics TPEditor Versions 1.97 and prior. An out-of-bounds read may be exploited by processing specially crafted project files. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application.	7.8	More Details
CVE-2020-0241	In NuPlayerStreamListener of NuPlayerStreamListener.cpp, there is possible memory corruption 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-8.0 Android-8.1 Android-9 Android-10Android ID: A-151456667	7.8	More Details
CVE-2020-6070	An exploitable code execution vulnerability exists in the file system checking functionality of fsck.f2fs 1.12.0. A specially crafted f2fs file can cause a logic flaw and out-of-bounds heap operations, resulting in code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2020-0259	In android_verity_ctr of dm-android-verity.c, there is a possible way to modify a dm-verity protected filesystem due to improperly used crypto. 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-157941353References: N/A	7.8	More Details
CVE-2020-0257	In SpecializeCommon of com_android_internal_os_Zygote.cpp, there is a permissions bypass due to an incomplete cleanup. This could lead to local escalation of privilege in isolated processes with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-156741968	7.8	More Details
CVE-2020-15657	Firefox could be made to load attacker-supplied DLL files from the installation directory. This required an attacker that is already capable of placing files in the installation directory. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0243	In clearPropValue of MediaAnalyticsItem.cpp, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the media server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-8.0 Android-8.1Android ID: A-151644303	7.8	More Details
CVE-2020-0242	In reset of NuPlayerDriver.cpp, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the media server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-151643722	7.8	More Details
CVE-2020-9078	FusionCompute 8.0.0 have local privilege escalation vulnerability. A local, authenticated attacker could perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege and compromise the service.	7.8	More Details
CVE-2020-16207	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. Multiple heap-based buffer overflow vulnerabilities may be exploited by opening specially crafted project files that may overflow the heap, which may allow remote code execution, disclosure/modification of information, or cause the application to crash.	7.8	More Details
CVE-2020-16213	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. Processing specially crafted project files lacking proper validation of user supplied data may cause the system to write outside the intended buffer area, which may allow remote code execution, disclosure/modification of information, or cause the application to crash.	7.8	More Details
CVE-2020-16215	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. Processing specially crafted project files lacking proper validation of user supplied data may cause a stack-based buffer overflow, which may allow remote code execution, disclosure/modification of information, or cause the application to crash.	7.8	More Details
CVE-2020-16229	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. Processing specially crafted project files lacking proper validation of user supplied data may cause a type confusion condition, which may allow remote code execution, disclosure/modification of information, or cause the application to crash.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0108	In postNotification of ServiceRecord.java, there is a possible bypass of foreground process restrictions due to an uncaught exception. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.1 Android-9Android ID: A-140108616	7.8	More Details
CVE-2020-16217	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. A double free vulnerability caused by processing specially crafted project files may allow remote code execution, disclosure/modification of information, or cause the application to crash.	7.8	More Details
CVE-2020-15114	In etcd before versions 3.3.23 and 3.4.10, the etcd gateway is a simple TCP proxy to allow for basic service discovery and access. However, it is possible to include the gateway address as an endpoint. This results in a denial of service, since the endpoint can become stuck in a loop of requesting itself until there are no more available file descriptors to accept connections on the gateway.	7.7	More Details
CVE-2020-15827	In JetBrains ToolBox version 1.17 before 1.17.6856, the set of signature verifications omitted the jetbrains-toolbox.exe file.	7.5	More Details
CVE-2020-15823	JetBrains YouTrack before 2020.2.8873 is vulnerable to SSRF in the Workflow component.	7.5	More Details
CVE-2020-17478	ECDSA/EC/Point.pm in Crypt::Perl before 0.33 does not properly consider timing attacks against the EC point multiplication algorithm.	7.5	More Details
CVE-2020-12777	A function in Combodo iTop contains a vulnerability of Broken Access Control, which allows unauthorized attacker to inject command and disclose system information.	7.5	More Details
CVE-2019-19704	In JetBrains Upsource before 2020.1, information disclosure is possible because of an incorrect user matching algorithm.	7.5	More Details
CVE-2020-12780	A security misconfiguration exists in Combodo iTop, which can expose sensitive information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9528	Firmware developed by Shenzhen Hichip Vision Technology (V6 through V20), as used by many different vendors in millions of Internet of Things devices, suffers from cryptographic issues that allow remote attackers to access user session data, as demonstrated by eavesdropping on user video/audio streams, capturing credentials, and compromising devices. This affects products marketed under the following brand names: Accfly, Alptop, Anlink, Besdersec, BOAVISION, COOAU, CPVAN, Ctronics, D3D Security, Dericam, Elex System, Elite Security, ENSTER, ePGes, Escam, FLOUREON, GENBOLT, Hongjingtian (HJT), ICAMI, Iegeek, Jecurity, Jennov, KKMoon, LEFTEK, Loosafe, Luowice, Nesuniq, Nettoly, ProElite, QZT, Royallite, SDETER, SV3C, SY2L, Tenvis, ThinkValue, TOMLOV, TPTEK, WGCC, and ZILINK.	7.5	More Details
CVE-2020-9490	Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.	7.5	More Details
CVE-2019-7005	A vulnerability was discovered in the web interface component of IP Office that may potentially allow a remote, unauthenticated user with network access to gain sensitive information. Affected versions of IP Office include: 9.x, 10.0 through 10.1.0.7 and 11.0 through 11.0.4.2.	7.5	More Details
CVE-2020-11976	By crafting a special URL it is possible to make Wicket deliver unprocessed HTML templates. This would allow an attacker to see possibly sensitive information inside a HTML template that is usually removed during rendering. Affected are Apache Wicket versions 7.16.0, 8.8.0 and 9.0.0-M5	7.5	More Details
CVE-2020-15127	In Contour (Ingress controller for Kubernetes) before version 1.7.0, a bad actor can shut down all instances of Envoy, essentially killing the entire ingress data plane. GET requests to /shutdown on port 8090 of the Envoy pod initiate Envoy's shutdown procedure. The shutdown procedure includes flipping the readiness endpoint to false, which removes Envoy from the routing pool. When running Envoy (For example on the host network, pod spec hostNetwork=true), the shutdown manager's endpoint is accessible to anyone on the network that can reach the Kubernetes node that's running Envoy. There is no authentication in place that prevents a rogue actor on the network from shutting down Envoy via the shutdown manager endpoint. Successful exploitation of this issue will lead to bad actors shutting down all instances of Envoy, essentially killing the entire ingress data plane. This is fixed in version 1.7.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7298	Unexpected behavior violation in McAfee Total Protection (MTP) prior to 16.0.R26 allows local users to turn off real time scanning via a specially crafted object making a specific function call.	7.5	More Details
CVE-2020-16845	Go before 1.13.15 and 14.x before 1.14.7 can have an infinite read loop in ReadUvarint and ReadVarint in encoding/binary via invalid inputs.	7.5	More Details
CVE-2020-0254	There is a possible out of bounds read due to an incorrect bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-152647751	7.5	More Details
CVE-2020-16170	Use of Hard-coded Credentials in temi Robox OS prior to 120, temi Android app up to 1.3.7931 allows remote attackers to listen in on any ongoing calls between temi robots and their users if they can brute-force/guess a six-digit value via unspecified vectors.	7.5	More Details
CVE-2020-0251	There is a possible out of bounds read due to an incorrect bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-152647626	7.5	More Details
CVE-2020-17487	radare2 4.5.0 misparses signature information in PE files, causing a segmentation fault in r_x509_parse_algorithmidentifier in libr/util/x509.c. This is due to a malformed object identifier in IMAGE_DIRECTORY_ENTRY_SECURITY.	7.5	More Details
CVE-2020-17495	django-celery-results through 1.2.1 stores task results in the database. Among the data it stores are the variables passed into the tasks. The variables may contain sensitive cleartext information that does not belong unencrypted in the database.	7.5	More Details
CVE-2020-11993	Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.	7.5	More Details
CVE-2020-13175	The Management Interface of the Teradici Cloud Access Connector and Cloud Access Connector Legacy for releases prior to April 20, 2020 (v15 and earlier for Cloud Access Connector) contains a local file inclusion vulnerability which allows an unauthenticated remote attacker to leak LDAP credentials via a specially crafted HTTP request.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15647	A Content Provider in Firefox for Android allowed local files accessible by the browser to be read by a remote webpage, leading to sensitive data disclosure, including cookies for other origins. This vulnerability affects Firefox for < Android.	7.4	More Details
CVE-2020-12778	Combodo iTop does not validate inputted parameters, attackers can inject malicious commands and launch XSS attack.	7.4	More Details
CVE-2020-17366	An issue was discovered in NLnet Labs Routinator 0.1.0 through 0.7.1. It allows remote attackers to bypass intended access restrictions or to cause a denial of service on dependent routing systems by strategically withholding RPKI Route Origin Authorisation ".roa" files or X509 Certificate Revocation List files from the RPKI relying party's view.	7.4	More Details
CVE-2020-17452	flatCore before 1.5.7 allows upload and execution of a .php file by an admin.	7.2	More Details
CVE-2020-15138	Prism is vulnerable to Cross-Site Scripting. The easing preview of the Previewers plugin has an XSS vulnerability that allows attackers to execute arbitrary code in Safari and Internet Explorer. This impacts all Safari and Internet Explorer users of Prism >=v1.1.0 that use the _Previewers_ plugin (>=v1.10.0) or the _Previewer: Easing_ plugin (v1.1.0 to v1.9.0). This problem is fixed in version 1.21.0. To workaround the issue without upgrading, disable the easing preview on all impacted code blocks. You need Prism v1.10.0 or newer to apply this workaround.	7.1	More Details
CVE-2020-14296	Red Hat CloudForms 4.7 and 5 was vulnerable to Server-Side Request Forgery (SSRF) flaw. With the access to add Ansible Tower provider, an attacker could scan and attack systems from the internal network which are not normally accessible.	7.1	More Details
CVE-2020-9404	In PACTware before 4.1 SP6 and 5.x before 5.0.5.31, passwords are stored in an insecure manner, and may be modified by an attacker with no knowledge of the current passwords.	7.1	More Details
CVE-2020-15702	TOCTOU Race Condition vulnerability in apport allows a local attacker to escalate privileges and execute arbitrary code. An attacker may exit the crashed process and exploit PID recycling to spawn a root process with the same PID as the crashed process, which can then be used to escalate privileges. Fixed in 2.20.1-0ubuntu2.24, 2.20.9 versions prior to 2.20.9-0ubuntu7.16 and 2.20.11 versions prior to 2.20.11-0ubuntu27.6. Was ZDI-CAN-11234.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0238	In updatePreferenceIntents of AccountTypePreferenceLoader, there is a possible confused deputy attack due to a race condition. This could lead to local escalation of privilege and launching privileged activities with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-150946634	7.0	More Details
CVE-2020-7460	In FreeBSD 12.1-STABLE before r363918, 12.1-RELEASE before p8, 11.4-STABLE before r363919, 11.4-RELEASE before p2, and 11.3-RELEASE before p12, the sendmsg system call in the compat32 subsystem on 64-bit platforms has a time-of-check to time-of-use vulnerability allowing a mailcious userspace program to modify control message headers after they were validation.	7.0	More Details
CVE-2020-0256	In LoadPartitionTable of gpt.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege when inserting a malicious USB device, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-152874864	6.8	More Details
CVE-2020-12779	Combodo iTop contains a stored Cross-site Scripting vulnerability, which can be attacked by uploading file with malicious script.	6.8	More Details
CVE-2020-7459	In FreeBSD 12.1-STABLE before r362166, 12.1-RELEASE before p8, 11.4-STABLE before r362167, 11.4-RELEASE before p2, and 11.3-RELEASE before p12, missing length validation code common to mulitple USB network drivers allows a malicious USB device to write beyond the end of an allocated network packet buffer.	6.8	More Details
CVE-2019-17339	The VirtualRouter component of TIBCO Software Inc.'s TIBCO Silver Fabric contains a vulnerability that theoretically allows an attacker to inject scripts via URLs. The attacker could theoretically social engineer an authenticated user into submitting the URL, thus executing the script on the affected system with the privileges of the user. Affected releases are TIBCO Software Inc.'s TIBCO Silver Fabric: versions 6.0.0 and below.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9244	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5),Versions earlier than 10.1.0.270(C635E3R1P5),Versions earlier than 10.1.0.273(C636E7R2P4);HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged	6.8	More Details
CVE-2020-8607	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability.	6.7	More Details
CVE-2020-13178	A function in the Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows prior to version 20.04.1 does not properly validate the signature of an external binary, which could allow an attacker to gain elevated privileges via execution in the context of the PCoIP Agent process.	6.7	More Details
CVE-2020-14344	An integer overflow leading to a heap-buffer overflow was found in The X Input Method (XIM) client was implemented in libX11 before version 1.6.10. As per upstream this is security relevant when setuid programs call XIM client functions while running with elevated privileges. No such programs are shipped with Red Hat Enterprise Linux.	6.7	More Details
CVE-2020-15658	The code for downloading files did not properly take care of special characters, which led to an attacker being able to cut off the file ending at an earlier position, leading to a different file type being downloaded than shown in the dialog. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15661	A rogue webpage could override the injected WKUserScript used by the logins autofill, this exploit could result in leaking a password for the current domain. This vulnerability affects Firefox for iOS < 28.	6.5	More Details
CVE-2020-15655	A redirected HTTP request which is observed or modified through a web extension could bypass existing CORS checks, leading to potential disclosure of cross-origin information. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.	6.5	More Details
CVE-2020-15654	When in an endless loop, a website specifying a custom cursor using CSS could make it look like the user is interacting with the user interface, when they are not. This could lead to a perceived broken state, especially when interactions with existing browser dialogs and warnings do not work. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.	6.5	More Details
CVE-2020-15653	An iframe sandbox element with the allow-popups flag could be bypassed when using noopener links. This could have led to security issues for websites relying on sandbox configurations that allowed popups and hosted arbitrary content. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.	6.5	More Details
CVE-2020-15652	By observing the stack trace for JavaScript errors in web workers, it was possible to leak the result of a cross-origin redirect. This applied only to content that can be parsed as script. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1.	6.5	More Details
CVE-2020-15648	Using object or embed tags, it was possible to frame other websites, even if they disallowed framing using the X-Frame-Options header. This vulnerability affects Thunderbird < 78 and Firefox < 78.0.2.	6.5	More Details
CVE-2020-4485	IBM QRadar 7.2.0 through 7.2.9 could allow an authenticated user to disable the Wincollect service which could aid an attacker in bypassing security mechanisms in future attacks. IBM X-Force ID: 181860.	6.5	More Details
CVE-2020-10779	Red Hat CloudForms 4.7 and 5 leads to insecure direct object references (IDOR) and functional level access control bypass due to missing privilege check. Therefore, if an attacker knows the right criteria, it is possible to access some sensitive data within the CloudForms.	6.5	More Details
CVE-2020-15662	A rogue webpage could override the injected WKUserScript used by the download feature, this exploit could result in the user downloading an unintended file. This vulnerability affects Firefox for iOS < 28.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18112	Affected versions of Atlassian Fisheye allow remote attackers to view the HTTP password of a repository via an Information Disclosure vulnerability in the logging feature. The affected versions are before version 4.8.3.	6.5	More Details
CVE-2020-15821	In JetBrains YouTrack before 2020.2.6881, a user without permission is able to create an article draft.	6.5	More Details
CVE-2020-15106	In etcd before versions 3.3.23 and 3.4.10, a large slice causes panic in decodeRecord method. The size of a record is stored in the length field of a WAL file and no additional validation is done on this data. Therefore, it is possible to forge an extremely large frame size that can unintentionally panic at the expense of any RAFT participant trying to decode the WAL.	6.5	More Details
CVE-2020-16168	Origin Validation Error in temi Robox OS prior to 120, temi Android app up to 1.3.7931 allows remote attackers to access the REST API and MQTT broker used by the temi and send it custom data/requests via unspecified vectors.	6.5	More Details
CVE-2020-5412	Spring Cloud Netflix, versions 2.2.x prior to 2.2.4, versions 2.1.x prior to 2.1.6, and older unsupported versions allow applications to use the Hystrix Dashboard proxy.stream endpoint to make requests to any server reachable by the server hosting the dashboard. A malicious user, or attacker, can send a request to other servers that should not be exposed publicly.	6.5	More Details
CVE-2020-15136	In ectd before versions 3.4.10 and 3.3.23, gateway TLS authentication is only applied to endpoints detected in DNS SRV records. When starting a gateway, TLS authentication will only be attempted on endpoints identified in DNS SRV records for a given domain, which occurs in the discoverEndpoints function. No authentication is performed against endpoints provided in the --endpoints flag. This has been fixed in versions 3.4.10 and 3.3.23 with improved documentation and deprecation of the functionality.	6.5	More Details
CVE-2020-15057	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to denial-of-service the device via long input values.	6.5	More Details
CVE-2020-15061	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to denial-of-service the device via long input values.	6.5	More Details
CVE-2020-15065	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to denial-of-service the device via long input values.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15828	In JetBrains TeamCity before 2020.1.1, project parameter values can be retrieved by a user without appropriate permissions.	6.5	More Details
CVE-2020-15112	In etcd before versions 3.3.23 and 3.4.10, it is possible to have an entry index greater then the number of entries in the ReadAll method in wal/wal.go. This could cause issues when WAL entries are being read during consensus as an arbitrary etcd consensus participant could go down from a runtime panic when reading the entry.	6.5	More Details
CVE-2020-7029	A Cross-Site Request Forgery (CSRF) vulnerability was discovered in the System Management Interface Web component of Avaya Aura Communication Manager and Avaya Aura Messaging. This vulnerability could allow an unauthenticated remote attacker to perform Web administration actions with the privileged level of the authenticated user. Affected versions of Communication Manager are 7.0.x, 7.1.x prior to 7.1.3.5 and 8.0.x. Affected versions of Messaging are 7.0.x, 7.1 and 7.1 SP1.	6.4	More Details
CVE-2020-13293	In GitLab before 13.0.12, 13.1.6 and 13.2.3 using a branch with a hexadecimal name could override an existing hash.	6.3	More Details
CVE-2020-10780	Red Hat CloudForms 4.7 and 5 is affected by CSV Injection flaw, a crafted payload stays dormant till a victim export as CSV and opens the file with Excel. Once the victim opens the file, the formula executes, triggering any number of possible events. While this is strictly not an flaw that affects the application directly, attackers could use the loosely validated parameters to trigger several attack possibilities.	6.3	More Details
CVE-2020-8918	An improperly initialized 'migrationAuth' value in Google's go-tpm TPM1.2 library versions prior to 0.3.0 can lead an eavesdropping attacker to discover the auth value for a key created with CreateWrapKey. An attacker listening in on the channel can collect both 'encUsageAuth' and 'encMigrationAuth', and then can calculate 'usageAuth ^ encMigrationAuth' as the 'migrationAuth' can be guessed for all keys created with CreateWrapKey. TPM2.0 is not impacted by this. We recommend updating your library to 0.3.0 or later, or, if you cannot update, to call CreateWrapKey with a random 20-byte value for 'migrationAuth'.	6.3	More Details
CVE-2020-4533	IBM Jazz Reporting Service 6.0.6, 6.0.6.1, and 7.0 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: 182717.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16275	A cross-site scripting (XSS) vulnerability in the Credential Manager component in SAINT Security Suite 8.0 through 9.8.20 could allow arbitrary script to run in the context of a logged-in user when the user clicks on a specially crafted link.	6.1	More Details
CVE-2020-15071	content/content.blueprintsevents.php in Symphony CMS 3.0.0 allows XSS via fields['name'] to appendSubheading.	6.1	More Details
CVE-2020-13176	The Management Interface of the Teradici Cloud Access Connector and Cloud Access Connector Legacy for releases prior to April 24, 2020 (v16 and earlier for the Cloud Access Connector) contains a stored cross-site scripting (XSS) vulnerability which allows a remote unauthenticated attacker to poison log files with malicious JavaScript via the login page which is executed when an administrator views the logs within the application.	6.1	More Details
CVE-2020-15907	In Mahara 19.04 before 19.04.6, 19.10 before 19.10.4, and 20.04 before 20.04.1, certain places could execute file or folder names containing JavaScript.	6.1	More Details
CVE-2020-13174	The web server in the Teradici Managament console versions 20.04 and 20.01.1 did not properly set the X-Frame-Options HTTP header, which could allow an attacker to trick a user into clicking a malicious link via clickjacking.	6.1	More Details
CVE-2020-17476	Mibew Messenger before 3.2.7 allows XSS via a crafted user name.	6.1	More Details
CVE-2020-17364	USVN (aka User-friendly SVN) before 1.0.9 allows XSS via SVN logs.	6.1	More Details
CVE-2020-9036	Jeedom through 4.0.38 allows XSS.	6.1	More Details
CVE-2020-16254	The Chartkick gem through 3.3.2 for Ruby allows Cascading Style Sheets (CSS) Injection (without attribute).	6.1	More Details
CVE-2020-16278	A cross-site scripting (XSS) vulnerability in the Permissions component in SAINT Security Suite 8.0 through 9.8.20 could allow arbitrary script to run in the context of a logged-in user when the user clicks on a specially crafted link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8025	A Incorrect Execution-Assigned Permissions vulnerability in the permissions package of SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 15; openSUSE Leap 15.1, openSUSE Tumbleweed sets the permissions for some of the directories of the pcp package to unintended settings. This issue affects: SUSE Linux Enterprise Server 12-SP4 permissions versions prior to 20170707-3.24.1. SUSE Linux Enterprise Server 15-LTSS permissions versions prior to 20180125-3.27.1. SUSE Linux Enterprise Server for SAP 15 permissions versions prior to 20180125-3.27.1. openSUSE Leap 15.1 permissions versions prior to 20181116-lp151.4.24.1. openSUSE Tumbleweed permissions versions prior to 20200624.	6.1	More Details
CVE-2020-15830	JetBrains TeamCity before 2019.2.3 is vulnerable to stored XSS in the administration UI.	6.1	More Details
CVE-2020-4541	IBM Jazz Reporting Service 7.0 and 7.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 183039.	6.1	More Details
CVE-2020-13819	Extreme EAC Appliance 8.4.1.24 allows unauthenticated reflected XSS via a parameter in a GET request.	6.1	More Details
CVE-2020-16192	LimeSurvey 4.3.2 allows reflected XSS because application/controllers/LSBaseController.php lacks code to validate parameters.	6.1	More Details
CVE-2020-15831	JetBrains TeamCity before 2019.2.3 is vulnerable to reflected XSS in the administration UI.	6.1	More Details
CVE-2020-17480	TinyMCE before 4.9.7 and 5.x before 5.1.4 allows XSS in the core parser, the paste plugin, and the visualchars plugin by using the clipboard or APIs to insert content into the editor.	6.1	More Details
CVE-2020-4539	IBM Jazz Reporting Service 6.0.2, 6.0.6, 6.0.6.1, 7.0, and 7.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10778	In Red Hat CloudForms 4.7 and 5, the read only widgets can be edited by inspecting the forms and dropping the disabled attribute from the fields since there is no server-side validation. This business logic flaw violate the expected behavior.	6.0	More Details
CVE-2020-9526	CS2 Network P2P through 3.x, as used in millions of Internet of Things devices, suffers from an information exposure flaw that exposes user session data to supernodes in the network, as demonstrated by passively eavesdropping on user video/audio streams, capturing credentials, and compromising devices.	5.9	More Details
CVE-2020-16248	Prometheus Blackbox Exporter through 0.17.0 allows /probe?target= SSRF. NOTE: follow-on discussion suggests that this might plausibly be interpreted as both intended functionality and also a vulnerability	5.8	More Details
CVE-2020-15115	etcd before versions 3.3.23 and 3.4.10 does not perform any password length validation, which allows for very short passwords, such as those with a length of one. This may allow an attacker to guess or brute-force users' passwords with little computational effort.	5.8	More Details
CVE-2020-12781	Combodo iTop contains a cross-site request forgery (CSRF) vulnerability, attackers can execute specific commands via malicious site request forgery.	5.7	More Details
CVE-2020-15113	In etcd before versions 3.3.23 and 3.4.10, certain directory paths are created (etcd data directory and the directory path when provided to automatically generate self-signed certificates for TLS connections with clients) with restricted access permissions (700) by using the os.MkdirAll. This function does not perform any permission checks when a given directory path exists already. A possible workaround is to ensure the directories have the desired permission (700).	5.7	More Details
CVE-2020-8911	A padding oracle vulnerability exists in the AWS S3 Crypto SDK for GoLang versions prior to V2. The SDK allows users to encrypt files with AES-CBC without computing a Message Authentication Code (MAC), which then allows an attacker who has write access to the target's S3 bucket and can observe whether or not an endpoint with access to the key can decrypt a file, they can reconstruct the plaintext with (on average) 128*length (plaintext) queries to the endpoint, by exploiting CBC's ability to manipulate the bytes of the next block and PKCS5 padding errors. It is recommended to update your SDK to V2 or later, and re-encrypt your files.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15701	An unhandled exception in check_ignored() in apport/report.py can be exploited by a local attacker to cause a denial of service. If the mtime attribute is a string value in apport-ignore.xml, it will trigger an unhandled exception, resulting in a crash. Fixed in 2.20.1-0ubuntu2.24, 2.20.9-0ubuntu7.16, 2.20.11-0ubuntu27.6.	5.5	More Details
CVE-2020-14347	A flaw was found in the way xserver memory was not properly initialized. This could leak parts of server memory to the X client. In cases where Xorg server runs with elevated privileges, this could result in possible ASLR bypass. Xorg-server before version 1.20.9 is vulnerable.	5.5	More Details
CVE-2020-9403	In PACTware before 4.1 SP6 and 5.x before 5.0.5.31, passwords are stored in a recoverable format, and may be retrieved by any user with access to the PACTware workstation.	5.5	More Details
CVE-2020-0248	In postInstantAppNotif of InstantAppNotifier.java, there is a possible permission bypass due to a PendingIntent error. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-154627439	5.5	More Details
CVE-2020-11937	In whoopsie, parse_report() from whoopsie.c allows a local attacker to cause a denial of service via a crafted file. The DoS is caused by resource exhaustion due to a memory leak. Fixed in 0.2.52.5ubuntu0.5, 0.2.62ubuntu0.5 and 0.2.69ubuntu0.1.	5.5	More Details
CVE-2020-0247	In Threshold::getHistogram of ImageProcessHelper.java, there is a possible crash loop due to an uncaught exception. This could lead to local denial of service with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-8.0 Android-8.1Android ID: A-156087409	5.5	More Details
CVE-2020-16211	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. An out-of-bounds read vulnerability may be exploited by processing specially crafted project files, which may allow an attacker to read information.	5.5	More Details
CVE-2020-0239	In getDocumentMetadata of DocumentsContract.java, there is a possible disclosure of location metadata from a file due to a permissions bypass. This could lead to local information disclosure from a file (eg. a photo) containing location metadata with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-151095863	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7817	MyBrowserPlus downloads the files needed to run the program through the setup file (Setup.inf). At this time, there is a vulnerability in downloading arbitrary files due to insufficient integrity verification of the files.	5.5	More Details
CVE-2020-0250	In requestCellInfoUpdateInternal of PhoneInterfaceManager.java, there is a missing permission check. This could lead to local information disclosure of location data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-154934934	5.5	More Details
CVE-2020-0249	In postInstantAppNotif of InstantAppNotifier.java, there is a possible permission bypass due to a PendingIntent error. This could lead to local information disclosure 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-154719656	5.5	More Details
CVE-2020-0258	In stopZygoteLocked of AppZygote.java, there is an insufficient cleanup. This could lead to local information disclosure in the application that is started next with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-157598956	5.5	More Details
CVE-2020-8229	A memory leak in the OCUtil.dll library used by Nextcloud Desktop Client 2.6.4 can lead to a DoS against the host system.	5.5	More Details
CVE-2020-13179	Broker Protocol messages in Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows prior to 20.04.1 are not cleaned up in server memory, which may allow an attacker to read confidential information from a memory dump via forcing a crashing during the single sign-on procedure.	5.5	More Details
CVE-2020-9243	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a denial of service vulnerability. The system does not properly limit the depth of recursion, an attacker should trick the user installing and execute a malicious application. Successful exploit could cause a denial of service condition.	5.5	More Details
CVE-2020-15649	Given an installed malicious file picker application, an attacker was able to steal and upload local files of their choosing, regardless of the actually files picked. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.11.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15650	Given an installed malicious file picker application, an attacker was able to overwrite local files and thus overwrite Firefox settings (but not access the previous profile). *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.11.	5.5	More Details
CVE-2020-9245	HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) have a denial of service vulnerability. Certain system configuration can be modified because of improper authorization. The attacker could trick the user installing and executing a malicious application, successful exploit could cause a denial of service condition of PHONE function.	5.5	More Details
CVE-2020-13295	For GitLab Runner before 13.0.12, 13.1.6, 13.2.3, by replacing dockerd with a malicious server, the Shared Runner is susceptible to SSRF.	5.4	More Details
CVE-2020-10777	A cross-site scripting flaw was found in Report Menu feature of Red Hat CloudForms 4.7 and 5. An attacker could use this flaw to execute a stored XSS attack on an application administrator using CloudForms.	5.4	More Details
CVE-2020-15597	SOPlanning 1.46.01 allows persistent XSS via the Project Name, Statutes Comment, Places Comment, or Resources Comment field.	5.4	More Details
CVE-2020-15818	In JetBrains YouTrack before 2020.2.8527, the subtasks workflow could disclose issue existence.	5.3	More Details
CVE-2020-15132	In Sulu before versions 1.6.35, 2.0.10, and 2.1.1, when the "Forget password" feature on the login screen is used, Sulu asks the user for a username or email address. If the given string is not found, a response with a `400` error code is returned, along with a error message saying that this user name does not exist. This enables attackers to retrieve valid usernames. Also, the response of the "Forgot Password" request returns the email address to which the email was sent, if the operation was successful. This information should not be exposed, as it can be used to gather email addresses. This problem was fixed in versions 1.6.35, 2.0.10 and 2.1.1.	5.3	More Details
CVE-2020-15819	JetBrains YouTrack before 2020.2.10643 was vulnerable to SSRF that allowed scanning internal ports.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15820	In JetBrains YouTrack before 2020.2.6881, the markdown parser could disclose hidden file existence.	5.3	More Details
CVE-2020-11985	IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.	5.3	More Details
CVE-2020-15829	In JetBrains TeamCity before 2019.2.3, password parameters could be disclosed via build logs.	5.3	More Details
CVE-2020-17451	flatCore before 1.5.7 allows XSS by an admin via the acp/acp.php?tn=pages&sub=edit&editpage=1 page_linkname, page_title, page_content, or page_extracontent parameter, or the acp/acp.php?tn=system&sub=sys_pref prefs_pagename, prefs_pagetitle, or prefs_pagesubtitle parameter.	4.8	More Details
CVE-2020-17489	An issue was discovered in certain configurations of GNOME gnome-shell through 3.36.4. When logging out of an account, the password box from the login dialog reappears with the password still visible. If the user had decided to have the password shown in cleartext at login time, it is then visible for a brief moment upon a logout. (If the password were never shown in cleartext, only the password length is revealed.)	4.3	More Details
CVE-2020-15056	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name.	4.3	More Details
CVE-2020-15651	A unicode RTL order character in the downloaded file name can be used to change the file's name during the download UI flow to change the file extension. This vulnerability affects Firefox for iOS < 28.	4.3	More Details
CVE-2020-14313	An information disclosure vulnerability was found in Red Hat Quay in versions before 3.3.1. This flaw allows an attacker who can create a build trigger in a repository, to disclose the names of robot accounts and the existence of private repositories within any namespace.	4.3	More Details
CVE-2020-15060	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15826	In JetBrains TeamCity before 2020.1, users are able to assign more permissions than they have.	4.3	More Details
CVE-2020-15064	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name.	4.3	More Details
CVE-2020-16252	The Field Test gem 0.2.0 through 0.3.2 for Ruby allows CSRF.	4.3	More Details
CVE-2020-13294	In GitLab before 13.0.12, 13.1.6 and 13.2.3, access grants were not revoked when a user revoked access to an application.	4.2	More Details
CVE-2020-16092	In QEMU through 5.0.0, an assertion failure can occur in the network packet processing. This issue affects the e1000e and vmxnet3 network devices. A malicious guest user/process could use this flaw to abort the QEMU process on the host, resulting in a denial of service condition in net_tx_pkt_add_raw_fragment in hw/net/net_tx_pkt.c.	3.8	More Details
CVE-2020-4243	IBM Security Identity Governance and Intelligence 5.2.6 Virtual Appliance could allow a remote attacker to obtain sensitive information using man in the middle techniques due to not properly invalidating session tokens. IBM X-Force ID: 175420.	3.7	More Details
CVE-2020-8912	A vulnerability in the in-band key negotiation exists in the AWS S3 Crypto SDK for GoLang versions prior to V2. An attacker with write access to the targeted bucket can change the encryption algorithm of an object in the bucket, which can then allow them to change AES-GCM to AES-CTR. Using this in combination with a decryption oracle can reveal the authentication key used by AES-GCM as decrypting the GMAC tag leaves the authentication key recoverable as an algebraic equation. It is recommended to update your SDK to V2 or later, and re-encrypt your files.	2.5	More Details
CVE-2020-16636	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17447	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-15139. Reason: This candidate is a duplicate of CVE-2020-15139. Notes: All CVE users should reference CVE-2020-15139 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details