SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 08 July 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-2020-15468	Persian VIP Download Script 1.0 allows SQL Injection via the cart_edit.php active parameter.	9.8	More Details
CVE-2020-15506	An authentication bypass vulnerability in MobileIron Core & Connector versions 10.3.0.3 and earlier, 10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4.0.3, 10.5.1.0, 10.5.2.0 and 10.6.0.0 that allows remote attackers to bypass authentication mechanisms via unspecified vectors.	9.8	More Details
CVE-2020-15539	SQL injection can occur in We-com Municipality portal CMS 2.1.x via the cerca/ keywords field.	9.8	More Details
CVE-2020-15540	We-com OpenData CMS 2.0 allows SQL Injection via the username field on the administrator login page.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15541	SolarWinds Serv-U FTP server before 15.2.1 allows remote command execution.	9.8	More Details
CVE-2020-15542	SolarWinds Serv-U FTP server before 15.2.1 mishandles the CHMOD command.	9.8	More Details
CVE-2020-15543	SolarWinds Serv-U FTP server before 15.2.1 does not validate an argument path.	9.8	More Details
CVE-2020-5368	Dell EMC VxRail versions 4.7.410 and 4.7.411 contain an improper authentication vulnerability. A remote unauthenticated attacker may exploit this vulnerability to obtain sensitive information in an encrypted form.	9.8	More Details
CVE-2020-15505	A remote code execution vulnerability in MobileIron Core & Connector versions 10.3.0.3 and earlier, 10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4.0.3, 10.5.1.0, 10.5.2.0 and 10.6.0.0; and Sentry versions 9.7.2 and earlier, and 9.8.0; and Monitor and Reporting Database (RDB) version 2.0.0.1 and earlier that allows remote attackers to execute arbitrary code via unspecified vectors.	9.8	More Details
CVE-2020-5595	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a buffer overflow vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	9.8	More Details
CVE-2020-14172	This issue exists to document that a security improvement in the way that Jira Server and Data Center use velocity templates has been implemented. The way in which velocity templates were used in Atlassian Jira Server and Data Center in affected versions allowed remote attackers to achieve remote code execution via insecure deserialization, if they were able to exploit a server side template injection vulnerability. The affected versions are before version 7.13.0, from version 8.0.0 before 8.5.0, and from version 8.6.0 before version 8.8.1.	9.8	More Details
CVE-2020-5599	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains an improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15367	Venki Supravizio BPM 10.1.2 does not limit the number of authentication attempts. An unauthenticated user may exploit this vulnerability to launch a brute-force authentication attack against the Login page.	9.8	More Details
CVE-2020-15350	RIOT 2020.04 has a buffer overflow in the base64 decoder. The decoding function base64_decode() uses an output buffer estimation function to compute the required buffer capacity and validate against the provided buffer size. The base64_estimate_decode_size() function calculates the expected decoded size with an arithmetic round-off error and does not take into account possible padding bytes. Due to this underestimation, it may be possible to craft base64 input that causes a buffer overflow.	9.8	More Details
CVE-2019-20896	WebChess 1.0 allows SQL injection via the messageFrom, gameID, opponent, messageID, or to parameter.	9.8	More Details
CVE-2020-12821	Gossipsub 1.0 does not properly resist invalid message spam, such as an eclipse attack or a sybil attack.	9.8	More Details
CVE-2020-8519	SQL injection with the search parameter in Records.php for phpzag live add edit delete data tables records with ajax php mysql	9.8	More Details
CVE-2020-8520	SQL injection in order and column parameters in Records.php for phpzag live add edit delete data tables records with ajax php mysql	9.8	More Details
CVE-2020-10282	The Micro Air Vehicle Link (MAVLink) protocol presents no authentication mechanism on its version 1.0 (nor authorization) whichs leads to a variety of attacks including identity spoofing, unauthorized access, PITM attacks and more. According to literature, version 2.0 optionally allows for package signing which mitigates this flaw. Another source mentions that MAVLink 2.0 only provides a simple authentication system based on HMAC. This implies that the flying system overall should add the same symmetric key into all devices of network. If not the case, this may cause a security issue, that if one of the devices and its symmetric key are compromised, the whole authentication system is not reliable.	9.8	More Details
CVE-2020-14092	The CodePeople Payment Form for PayPal Pro plugin before 1.1.65 for WordPress allows SQL Injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5902	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.	9.8	More Details
CVE-2020-13619	php/exec/escapeshellarg in Locutus PHP through 2.0.11 allows an attacker to achieve code execution.	9.8	More Details
CVE-2020-15474	In nDPI through 3.2, there is a stack overflow in extractRDNSequence in lib/protocols/tls.c.	9.8	More Details
CVE-2020-15475	In nDPI through 3.2, ndpi_reset_packet_line_info in lib/ndpi_main.c omits certain reinitialization, leading to a use-after-free.	9.8	More Details
CVE-2020-13380	openSIS before 7.4 allows SQL Injection.	9.8	More Details
CVE-2020-13381	openSIS through 7.4 allows SQL Injection.	9.8	More Details
CVE-2020-3297	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user.	9.8	More Details
CVE-2020-2500	This improper access control vulnerability in Helpdesk allows attackers to get control of QNAP Kayako service. Attackers can access the sensitive data on QNAP Kayako server with API keys. We have replaced the API key to mitigate the vulnerability, and already fixed the issue in Helpdesk 3.0.1 and later versions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8521	SQL injection with start and length parameters in Records.php for phpzag live add edit delete data tables records with ajax php mysql	9.8	More Details
CVE-2020-14056	Monsta FTP 2.10.1 or below is prone to a server-side request forgery vulnerability due to insufficient restriction of the web fetch functionality. This allows attackers to read arbitrary local files and interact with arbitrary third-party services.	9.8	More Details
CVE-2020-14057	Monsta FTP 2.10.1 or below allows external control of paths used in filesystem operations. This allows attackers to read and write arbitrary local files, allowing an attacker to gain remote code execution in common deployments.	9.8	More Details
CVE-2019-15310	An issue was discovered on various devices via the Linkplay firmware. There is WAN remote code execution without user interaction. An attacker could retrieve the AWS key from the firmware and obtain full control over Linkplay's AWS estate, including S3 buckets containing device firmware. When combined with an OS command injection vulnerability within the XML Parsing logic of the firmware update process, an attacker would be able to gain code execution on any device that attempted to update. Note that by default all devices tested had automatic updates enabled.	9.8	More Details
CVE-2019-15311	An issue was discovered on Zolo Halo devices via the Linkplay firmware. There is Zolo Halo LAN remote code execution. The Zolo Halo Bluetooth speaker had a GoAhead web server listening on the port 80. The /httpapi.asp endpoint of the GoAhead web server was also vulnerable to multiple command execution vulnerabilities.	9.8	More Details
CVE-2020-15489	An issue was discovered on Wavlink WL-WN530HG4 M30HG4.V5030.191116 devices. Multiple shell metacharacter injection vulnerabilities exist in CGI scripts, leading to remote code execution with root privileges.	9.8	More Details
CVE-2020-15490	An issue was discovered on Wavlink WL-WN530HG4 M30HG4.V5030.191116 devices. Multiple buffer overflow vulnerabilities exist in CGI scripts, leading to remote code execution with root privileges. (The set of affected scripts is similar to CVE-2020-12266.)	9.8	More Details
CVE-2020-5901	In NGINX Controller 3.3.0-3.4.0, undisclosed API endpoints may allow for a reflected Cross Site Scripting (XSS) attack. If the victim user is logged in as admin this could result in a complete compromise of the system.	9.6	More Details
CVE-2020-13382	openSIS through 7.4 has Incorrect Access Control.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15473	In nDPI through 3.2, the OpenVPN dissector is vulnerable to a heap-based buffer over-read in ndpi_search_openvpn in lib/protocols/openvpn.c.	9.1	More Details
CVE-2020-15472	In nDPI through 3.2, the H.323 dissector is vulnerable to a heap-based buffer over-read in ndpi_search_h323 in lib/protocols/h323.c, as demonstrated by a payload packet length that is too short.	9.1	More Details
CVE-2020-15471	In nDPI through 3.2, the packet parsing code is vulnerable to a heap-based buffer over-read in ndpi_parse_packet_line_info in lib/ndpi_main.c.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-4074	In PrestaShop from version 1.5.0.0 and before version 1.7.6.6, the authentication system is malformed and an attacker is able to forge requests and execute admin commands. The problem is fixed in 1.7.6.6.	8.9	More Details
CVE-2020-8188	We have recently released new version of UniFi Protect firmware v1.13.3 and v1.14.10 for Unifi Cloud Key Gen2 Plus and UniFi Dream Machine Pro/UNVR respectively that fixes vulnerabilities found on Protect firmware v1.13.2, v1.14.9 and prior according to the description below:View only users can run certain custom commands which allows them to assign themselves unauthorized roles and escalate their privileges.	8.8	More Details
CVE-2020-5904	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page.	8.8	More Details
CVE-2020-8163	The is a code injection vulnerability in versions of Rails prior to 5.0.1 that wouldallow an attacker who controlled the `locals` argument of a `render` call to perform a RCE.	8.8	More Details
CVE-2020-15515	The turn extension through 0.3.2 for TYPO3 allows Remote Code Execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15565	An issue was discovered in Xen through 4.13.x, allowing x86 Intel HVM guest OS users to cause a host OS denial of service or possibly gain privileges because of insufficient cache write-back under VT-d. When page tables are shared between IOMMU and CPU, changes to them require flushing of both TLBs. Furthermore, IOMMUs may be non-coherent, and hence prior to flushing IOMMU TLBs, a CPU cache also needs writing back to memory after changes were made. Such writing back of cached data was missing in particular when splitting large page mappings into smaller granularity ones. A malicious guest may be able to retain read/write DMA access to frames returned to Xen's free pool, and later reused for another purpose. Host crashes (leading to a Denial of Service) and privilege escalation cannot be ruled out. Xen versions from at least 3.2 onwards are affected. Only x86 Intel systems are affected. x86 AMD as well as Arm systems are not affected. Only x86 HVM guests using hardware assisted paging (HAP), having a passed through PCI device assigned, and having page table sharing enabled can leverage the vulnerability. Note that page table sharing will be enabled (by default) only if Xen considers IOMMU and CPU large page size support compatible.	8.8	More Details
CVE-2020-15518	VeeamFSR.sys in Veeam Availability Suite before 10 and Veeam Backup & Replication before 10 has no device object DACL, which allows unprivileged users to achieve total control over filesystem I/O requests.	8.8	More Details
CVE-2020-2211	Jenkins ElasticBox Jenkins Kubernetes CI/CD Plugin 1.3 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	8.8	More Details
CVE-2020-5900	In versions 3.0.0-3.4.0, 2.0.0-2.9.0, and 1.0.1, there is insufficient cross-site request forgery (CSRF) protections for the NGINX Controller user interface.	8.8	More Details
CVE-2020-5352	Dell EMC Data Protection Advisor 6.4, 6.5 and 18.1 contain an OS command injection vulnerability. A remote authenticated malicious user may exploit this vulnerability to execute arbitrary commands on the affected system.	8.8	More Details
CVE-2019-15312	An issue was discovered on Zolo Halo devices via the Linkplay firmware. There is a Zolo Halo DNS rebinding attack. The device was found to be vulnerable to DNS rebinding. Combined with one of the many /httpapi.asp endpoint command-execution security issues, the DNS rebinding attack could allow an attacker to compromise the victim device from the Internet.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6013	ZoneAlarm Firewall and Antivirus products before version 15.8.109.18436 allow an attacker who already has access to the system to execute code at elevated privileges through a combination of file permission manipulation and exploitation of Windows CVE-2020-00896 on unpatched systems.	8.8	More Details
CVE-2020-5372	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a vulnerability that exposes test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment.	8.6	More Details
CVE-2020-7284	Exposure of Sensitive Information in McAfee Network Security Management (NSM) prior to 10.1.7.7 allows local users to gain unauthorised access to the root account via execution of carefully crafted commands from the restricted command line interface (CLI).	8.6	More Details
CVE-2020-8161	A directory traversal vulnerability exists in rack < 2.2.0 that allows an attacker perform directory traversal vulnerability in the Rack::Directory app that is bundled with Rack which could result in information disclosure.	8.6	More Details
CVE-2020-7688	The issue occurs because tagName user input is formatted inside the exec function is executed without any checks.	8.4	More Details
CVE-2020-5906	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP.	8.1	More Details
CVE-2020-12119	Ledger Live before 2.7.0 does not handle Bitcoin's Replace-By-Fee (RBF). It increases the user's balance with the value of an unconfirmed transaction as soon as it is received (before the transaction is confirmed) and does not decrease the balance when it is canceled. As a result, users are exposed to basic double spending attacks, amplified double spending attacks, and DoS attacks without user consent.	8.1	More Details
CVE-2020-5371	Dell EMC Isilon OneFS versions 8.2.2 and earlier and Dell EMC PowerScale version 9.0.0 contain a file permissions vulnerability. An attacker, with network or local file access, could take advantage of insufficiently applied file permissions or gain unauthorized access to files.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9395	An issue was discovered on Realtek RTL8195AM, RTL8711AM, RTL8711AF, and RTL8710AF devices before 2.0.6. A stack-based buffer overflow exists in the client code that takes care of WPA2's 4-way-handshake via a malformed EAPOL-Key packet with a long keydata buffer.	8.0	More Details
CVE-2020-7821	Nexacro14/17 ExtCommonApiV13 Library under 2019.9.6 version contain a vulnerability that could allow remote attacker to execute arbitrary code by modifying the value of registry path. This can be leveraged for code execution by rebooting the victim’s PC	7.8	More Details
CVE-2020-7820	Nexacro14/17 ExtCommonApiV13 Library under 2019.9.6 version contain a vulnerability that could allow remote attacker to execute arbitrary code by setting the arguments to the vulnerable API. This can be leveraged for code execution by rebooting the victim’s PC	7.8	More Details
CVE-2019-8249	Adobe Acrobat and Reader versions 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2019-8066	Adobe Acrobat and Reader versions 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-15530	An issue was discovered in Valve Steam Client 2.10.91.91. The installer allows local users to gain NT AUTHORITY\SYSTEM privileges because some parts of %PROGRAMFILES(X86)%\Steam and/or %COMMONPROGRAMFILES(X86)%\Steam have weak permissions during a critical time window. An attacker can make this time window arbitrarily long by using opportunistic locks.	7.8	More Details
CVE-2020-15529	An issue was discovered in GOG Galaxy Client 2.0.17. Local escalation of privileges is possible when a user installs a game or performs a verify/repair operation. The issue exists because of weak file permissions and can be exploited by using opportunistic locks.	7.8	More Details
CVE-2020-9100	Earlier than HiSuite 10.1.0.500 have a DLL hijacking vulnerability. This vulnerability exists due to some DLL file is loaded by HiSuite improperly. And it allows an attacker to load this DLL file of the attacker's choosing.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15528	An issue was discovered in GOG Galaxy Client 2.0.17. Local escalation of privileges is possible when a user starts or uninstalls a game because of weak file permissions and missing file integrity checks.	7.8	More Details
CVE-2020-15523	In Python 3.6 through 3.6.10, 3.7 through 3.7.8, 3.8 through 3.8.4rc1, and 3.9 through 3.9.0b4 on Windows, a Trojan horse python3.dll might be used in cases where CPython is embedded in a native application. This occurs because python3X.dll may use an invalid search path for python3.dll loading (after Py_SetPath has been used). NOTE: this issue CANNOT occur when using python.exe from a standard (non-embedded) Python installation on Windows.	7.8	More Details
CVE-2020-9261	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a type confusion vulnerability. The system does not properly check and transform the type of certain variable, the attacker tricks the user into installing then running a crafted application, successful exploit could cause code execution.	7.8	More Details
CVE-2020-12498	mwe file parsing in Phoenix Contact PC Worx and PC Worx Express version 1.87 and earlier is vulnerable to out-of-bounds read remote code execution. Manipulated PC Worx projects could lead to a remote code execution due to insufficient input data validation.	7.8	More Details
CVE-2020-12497	PLCopen XML file parsing in Phoenix Contact PC Worx and PC Worx Express version 1.87 and earlier can lead to a stack-based overflow. Manipulated PC Worx projects could lead to a remote code execution due to insufficient input data validation.	7.8	More Details
CVE-2020-9262	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a use after free vulnerability. There is a condition exists that the system would reference memory after it has been freed, the attacker should trick the user into running a crafted application with high privilege, successful exploit could cause code execution.	7.8	More Details
CVE-2019-20419	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to execute arbitrary code via a DLL hijacking vulnerability in Tomcat. The affected versions are before version 8.5.5, and from version 8.6.0 before 8.7.2.	7.8	More Details
CVE-2019-8250	Adobe Acrobat and Reader versions 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6089	An exploitable code execution vulnerability exists in the ANI file format parser of Leadtools 20. A specially crafted ANI file can cause a buffer overflow resulting in remote code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2019-4676	IBM Security Identity Manager Virtual Appliance 7.0.2 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 171512.	7.8	More Details
CVE-2020-4076	In Electron before versions 7.2.4, 8.2.4, and 9.0.0-beta21, there is a context isolation bypass. Code running in the main world context in the renderer can reach into the isolated Electron context and perform privileged actions. Apps using contextIsolation are affected. This is fixed in versions 9.0.0-beta.21, 8.2.4 and 7.2.4.	7.8	More Details
CVE-2020-15567	An issue was discovered in Xen through 4.13.x, allowing Intel guest OS users to gain privileges or cause a denial of service because of non-atomic modification of a live EPT PTE. When mapping guest EPT (nested paging) tables, Xen would in some circumstances use a series of non-atomic bitfield writes. Depending on the compiler version and optimisation flags, Xen might expose a dangerous partially written PTE to the hardware, which an attacker might be able to race to exploit. A guest administrator or perhaps even an unprivileged guest user might be able to cause denial of service, data corruption, or privilege escalation. Only systems using Intel CPUs are vulnerable. Systems using AMD CPUs, and Arm systems, are not vulnerable. Only systems using nested paging (hap, aka nested paging, aka in this case Intel EPT) are vulnerable. Only HVM and PVH guests can exploit the vulnerability. The presence and scope of the vulnerability depends on the precise optimisations performed by the compiler used to build Xen. If the compiler generates (a) a single 64-bit write, or (b) a series of read-modify-write operations in the same order as the source code, the hypervisor is not vulnerable. For example, in one test build using GCC 8.3 with normal settings, the compiler generated multiple (unlocked) read-modify-write operations in source-code order, which did not constitute a vulnerability. We have not been able to survey compilers; consequently we cannot say which compiler(s) might produce vulnerable code (with which code-generation options). The source code clearly violates the C rules, and thus should be considered vulnerable.	7.8	More Details
CVE-2020-5899	In NGINX Controller 3.0.0-3.4.0, recovery code required to change a user's password is transmitted and stored in the database in plain text, which allows an attacker who can intercept the database connection or have read access to the database, to request a password reset using the email address of another registered user then retrieve the recovery code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4363	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 178960.	7.8	More Details
CVE-2020-5356	Dell PowerProtect Data Manager (PPDM) versions prior to 19.4 and Dell PowerProtect X400 versions prior to 3.2 contain an improper authorization vulnerability. A remote authenticated malicious user may download any file from the affected PowerProtect virtual machines.	7.7	More Details
CVE-2020-4077	In Electron before versions 7.2.4, 8.2.4, and 9.0.0-beta21, there is a context isolation bypass. Code running in the main world context in the renderer can reach into the isolated Electron context and perform privileged actions. Apps using both `contextIsolation` and `contextBridge` are affected. This is fixed in versions 9.0.0-beta.21, 8.2.4 and 7.2.4.	7.7	More Details
CVE-2020-15576	SolarWinds Serv-U File Server before 15.2.1 allows information disclosure via an HTTP response.	7.5	More Details
CVE-2020-5910	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, the Neural Autonomic Transport System (NATS) messaging services in use by the NGINX Controller do not require any form of authentication, so any successful connection would be authorized.	7.5	More Details
CVE-2020-14167	The MessageBundleResource resource in Jira Server and Data Center before version 7.13.4, from 8.5.0 before 8.5.5, from 8.8.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to impact the application's availability via an Denial of Service (DoS) vulnerability.	7.5	More Details
CVE-2020-15579	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Attackers can bypass Factory Reset Protection (FRP) via the KNOX API. The Samsung ID is SVE-2020-17318 (July 2020).	7.5	More Details
CVE-2020-15503	LibRaw before 0.20-RC1 lacks a thumbnail size range check. This affects decoders/unpack_thumb.cpp, postprocessing/mem_image.cpp, and utils/thumb_utils.cpp. For example, malloc(sizeof(libraw_processed_image_t)+T.tlength) occurs without validating T.tlength.	7.5	More Details
CVE-2020-12603	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier may consume excessive amounts of memory when proxying HTTP/2 requests or responses with many small (i.e. 1 byte) data frames.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14303	A flaw was found in the AD DC NBT server in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4. A samba user could send an empty UDP packet to cause the samba server to crash.	7.5	More Details
CVE-2020-7281	Privilege Escalation vulnerability in McAfee Total Protection (MTP) prior to 16.0.R26 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.	7.5	More Details
CVE-2020-5600	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a resource management error vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	7.5	More Details
CVE-2020-15466	In Wireshark 3.2.0 to 3.2.4, the GVCP dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-gvcp.c by ensuring that an offset increases in all situations.	7.5	More Details
CVE-2020-15476	In nDPI through 3.2, the Oracle protocol dissector has a heap-based buffer over-read in ndpi_search_oracle in lib/protocols/oracle.c.	7.5	More Details
CVE-2020-7282	Privilege Escalation vulnerability in McAfee Total Protection (MTP) before 16.0.R26 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.	7.5	More Details
CVE-2020-10745	A flaw was found in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4 in the way it processed NetBios over TCP/IP. This flaw allows a remote attacker could to cause the Samba server to consume excessive CPU use, resulting in a denial of service. This highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2020-7283	Privilege Escalation vulnerability in McAfee Total Protection (MTP) before 16.0.R26 allows local users to create and edit files via symbolic link manipulation in a location they would otherwise not have access to. This is achieved through running a malicious script or program on the target machine.	7.5	More Details
CVE-2020-15478	The Journal theme before 3.1.0 for OpenCart allows exposure of sensitive data via SQL errors.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15502	The DuckDuckGo application through 5.58.0 for Android, and through 7.47.1.0 for iOS, sends hostnames of visited web sites within HTTPS .ico requests to servers in the duckduckgo.com domain, which might make visit data available temporarily at a Potentially Unwanted Endpoint. NOTE: the vendor has stated "the favicon service adheres to our strict privacy policy.	7.5	More Details
CVE-2020-15574	SolarWinds Serv-U File Server before 15.2.1 mishandles the Same-Site cookie attribute, aka Case Number 00331893.	7.5	More Details
CVE-2020-13383	openSIS through 7.4 allows Directory Traversal.	7.5	More Details
CVE-2020-4420	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated attacker to cause a denial of service due a hang in the execution of a terminate command. IBM X-Force ID: 180076.	7.5	More Details
CVE-2020-15008	A SQLi exists in the probe code of all Connectwise Automate versions before 2020.7 or 2019.12. A SQL Injection in the probe implementation to save data to a custom table exists due to inadequate server side validation. As the code creates dynamic SQL for the insert statement and utilizes the user supplied table name with little validation, the table name can be modified to allow arbitrary update commands to be run. Usage of other SQL injection techniques such as timing attacks, it is possible to perform full data extraction as well. Patched in 2020.7 and in a hotfix for 2019.12.	7.5	More Details
CVE-2020-8663	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier may exhaust file descriptors and/or memory when accepting too many connections.	7.5	More Details
CVE-2020-15507	An arbitrary file reading vulnerability in MobileIron Core versions 10.3.0.3 and earlier, 10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4.0.3, 10.5.1.0, 10.5.2.0 and 10.6.0.0 that allows remote attackers to read files on the system via unspecified vectors.	7.5	More Details
CVE-2020-5596	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) does not properly manage sessions, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10281	This vulnerability applies to the Micro Air Vehicle Link (MAVLink) protocol and allows a remote attacker to gain access to sensitive information provided it has access to the communication medium. MAVLink is a header-based protocol that does not perform encryption to improve transfer (and reception speed) and efficiency by design. The increasing popularity of the protocol (used accross different autopilots) has led to its use in wired and wireless mediums through insecure communication channels exposing sensitive information to a remote attacker with ability to intercept network traffic.	7.5	More Details
CVE-2019-20894	Traefik 2.x, in certain configurations, allows HTTPS sessions to proceed without mutual TLS verification in a situation where ERR_BAD_SSL_CLIENT_AUTH_CERT should have occurred.	7.5	More Details
CVE-2020-12605	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier may consume excessive amounts of memory when processing HTTP/1.1 headers with long field names or requests with long URLs.	7.5	More Details
CVE-2020-12604	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier is susceptible to increased memory usage in the case where an HTTP/2 client requests a large payload but does not send enough window updates to consume the entire stream and does not reset the stream.	7.5	More Details
CVE-2020-5597	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a null pointer dereference vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	7.5	More Details
CVE-2020-5598	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains an improper access control vulnerability, which may which may allow a remote attacker tobypass access restriction and stop the network functions of the products or execute a malicious program via a specially crafted packet.	7.5	More Details
CVE-2020-3402	A vulnerability in the Java Remote Method Invocation (RMI) interface of Cisco Unified Customer Voice Portal (CVP) could allow an unauthenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because certain RMI listeners are not properly authenticated. An attacker could exploit this vulnerability by sending a crafted request to the affected listener. A successful exploit could allow the attacker to access sensitive information on an affected device.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5911	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, the NGINX Controller installer starts the download of Kubernetes packages from an HTTP URL On Debian/Ubuntu system.	7.3	More Details
CVE-2020-5907	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality.	7.2	More Details
CVE-2020-12736	Code42 environments with on-premises server versions 7.0.4 and earlier allow for possible remote code execution. When an administrator creates a local (non-SSO) user via a Code42-generated email, the administrator has the option to modify content for the email invitation. If the administrator entered template language code in the subject line, that code could be interpreted by the email generation services, potentially resulting in server-side code injection.	7.2	More Details
CVE-2020-15082	In PrestaShop from version 1.6.0.1 and before version 1.7.6.6, the dashboard allows rewriting all configuration variables. The problem is fixed in 1.7.6.6	7.1	More Details
CVE-2020-15096	In Electron before versions 6.1.1, 7.2.4, 8.2.4, and 9.0.0-beta21, there is a context isolation bypass, meaning that code running in the main world context in the renderer can reach into the isolated Electron context and perform privileged actions. Apps using "contextIsolation" are affected. There are no app-side workarounds, you must update your Electron version to be protected. This is fixed in versions 6.1.1, 7.2.4, 8.2.4, and 9.0.0-beta21.	6.8	More Details
CVE-2020-4075	In Electron before versions 7.2.4, 8.2.4, and 9.0.0-beta21, arbitrary local file read is possible by defining unsafe window options on a child window opened via window.open. As a workaround, ensure you are calling `event.preventDefault()` on all new-window events where the `url` or `options` is not something you expect. This is fixed in versions 9.0.0-beta.21, 8.2.4 and 7.2.4.	6.8	More Details
CVE-2020-9498	Apache Guacamole 1.1.0 and older may mishandle pointers involved inprocessing data received via RDP static virtual channels. If a userconnects to a malicious or compromised RDP server, a series ofspecially-crafted PDUs could result in memory corruption, possiblyallowing arbitrary code to be executed with the privileges of therunning guacd process.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15509	Nordic Semiconductor Android BLE Library through 2.2.1 and DFU Library through 1.10.4 for Android (as used by nRF Connect and other applications) can engage in unencrypted communication while showing the user that the communication is purportedly encrypted. The problem is in bond creation (e.g., internalCreateBond in BleManagerHandler).	6.5	More Details
CVE-2020-10730	A NULL pointer dereference, or possible use-after-free flaw was found in Samba AD LDAP server in versions before 4.10.17, before 4.11.11 and before 4.12.4. Although some versions of Samba shipped with Red Hat Enterprise Linux do not support Samba in AD mode, the affected code is shipped with the libldb package. This flaw allows an authenticated user to possibly trigger a use-after-free or NULL pointer dereference. The highest threat from this vulnerability is to system availability.	6.5	More Details
CVE-2020-15566	An issue was discovered in Xen through 4.13.x, allowing guest OS users to cause a host OS crash because of incorrect error handling in event-channel port allocation. The allocation of an event-channel port may fail for multiple reasons: (1) port is already in use, (2) the memory allocation failed, or (3) the port we try to allocate is higher than what is supported by the ABI (e.g., 2L or FIFO) used by the guest or the limit set by an administrator (max_event_channels in xl cfg). Due to the missing error checks, only (1) will be considered an error. All the other cases will provide a valid port and will result in a crash when trying to access the event channel. When the administrator configured a guest to allow more than 1023 event channels, that guest may be able to crash the host. When Xen is out-of-memory, allocation of new event channels will result in crashing the host rather than reporting an error. Xen versions 4.10 and later are affected. All architectures are affected. The default configuration, when guests are created with xl/libxl, is not vulnerable, because of the default event-channel limit.	6.5	More Details
CVE-2020-15564	An issue was discovered in Xen through 4.13.x, allowing Arm guest OS users to cause a hypervisor crash because of a missing alignment check in VCPUOP_register_vcpu_info. The hypercall VCPUOP_register_vcpu_info is used by a guest to register a shared region with the hypervisor. The region will be mapped into Xen address space so it can be directly accessed. On Arm, the region is accessed with instructions that require a specific alignment. Unfortunately, there is no check that the address provided by the guest will be correctly aligned. As a result, a malicious guest could cause a hypervisor crash by passing a misaligned address. A malicious guest administrator may cause a hypervisor crash, resulting in a Denial of Service (DoS). All Xen versions are vulnerable. Only Arm systems are vulnerable. x86 systems are not affected.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20418	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to prevent users from accessing the instance via an Application Denial of Service vulnerability in the /rendering/wiki endpoint. The affected versions are before version 8.8.0.	6.5	More Details
CVE-2020-8185	A denial of service vulnerability exists in Rails <6.0.3.2 that allowed an untrusted user to run any pending migrations on a Rails app running in production.	6.5	More Details
CVE-2020-15563	An issue was discovered in Xen through 4.13.x, allowing x86 HVM guest OS users to cause a hypervisor crash. An inverted conditional in x86 HVM guests' dirty video RAM tracking code allows such guests to make Xen de-reference a pointer guaranteed to point at unmapped space. A malicious or buggy HVM guest may cause the hypervisor to crash, resulting in Denial of Service (DoS) affecting the entire host. Xen versions from 4.8 onwards are affected. Xen versions 4.7 and earlier are not affected. Only x86 systems are affected. Arm systems are not affected. Only x86 HVM guests using shadow paging can leverage the vulnerability. In addition, there needs to be an entity actively monitoring a guest's video frame buffer (typically for display purposes) in order for such a guest to be able to leverage the vulnerability. x86 PV guests, as well as x86 HVM guests using hardware assisted paging (HAP), cannot leverage the vulnerability.	6.5	More Details
CVE-2019-14900	A flaw was found in Hibernate ORM in versions before 5.3.18, 5.4.18 and 5.5.0.Beta1. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SELECT or GROUP BY parts of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks.	6.5	More Details
CVE-2020-10760	A use-after-free flaw was found in all samba LDAP server versions before 4.10.17, before 4.11.11, before 4.12.4 used in a AC DC configuration. A Samba LDAP user could use this flaw to crash samba.	6.5	More Details
CVE-2020-15091	TenderMint from version 0.33.0 and before version 0.33.6 allows block proposers to include signatures for the wrong block. This may happen naturally if you start a network, have it run for some time and restart it (**without changing chainID**). A malicious block proposer (even with a minimal amount of stake) can use this vulnerability to completely halt the network. This issue is fixed in Tendermint 0.33.6 which checks all the signatures are for the block with 2/3+ majority before creating a commit.	6.5	More Details
CVE-2020-15600	An issue was discovered in CMSUno before 1.6.1. uno.php allows CSRF to change the admin password.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4376	IBM MQ, IBM MQ Appliance, IBM MQ for HPE NonStop 8.0.4 and 8.1.0 could allow an attacker to cause a denial of service caused by an error within the pubsub logic. IBM X-Force ID: 179081.	6.5	More Details
CVE-2020-5238	The table extension in GitHub Flavored Markdown before version 0.29.0.gfm.1 takes O(n * n) time to parse certain inputs. An attacker could craft a markdown table which would take an unreasonably long time to process, causing a denial of service. This issue does not affect the upstream cmark project. The issue has been fixed in version 0.29.0.gfm.1.	6.5	More Details
CVE-2020-3391	A vulnerability in Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to view sensitive information in clear text. The vulnerability is due to insecure storage of certain unencrypted credentials on an affected device. An attacker could exploit this vulnerability by viewing the network device configuration and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices.	6.5	More Details
CVE-2020-15079	In PrestaShop from version 1.5.0.0 and before version 1.7.6.6, there is improper access control in Carrier page, Module Manager and Module Positions. The problem is fixed in version 1.7.6.6	6.4	More Details
CVE-2020-1839	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a race condition vulnerability. There is a timing window exists in which certain pointer members can be modified by another process that is operating concurrently, an attacker should trick the user into running a crafted application with high privilege, successful exploit could cause code execution.	6.3	More Details
CVE-2020-7691	In all versions of the package jspdf, it is possible to use <<script>script> in order to go over the filtering regex.	6.3	More Details
CVE-2020-13653	An XSS vulnerability exists in the Webmail component of Zimbra Collaboration Suite before 8.8.15 Patch 11. It allows an attacker to inject executable JavaScript into the account name of a user's profile. The injected code can be reflected and executed when changing an e-mail signature.	6.1	More Details
CVE-2020-5903	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7690	All affected versions <2.0.0 of package jspdf are vulnerable to Cross-site Scripting (XSS). It is possible to inject JavaScript code via the html method.	6.1	More Details
CVE-2020-15562	An issue was discovered in Roundcube Webmail before 1.2.11, 1.3.x before 1.3.14, and 1.4.x before 1.4.7. It allows XSS via a crafted HTML e-mail message, as demonstrated by a JavaScript payload in the xmlns (aka XML namespace) attribute of a HEAD element when an SVG element exists.	6.1	More Details
CVE-2020-15538	XSS can occur in We-com Municipality portal CMS 2.1.x via the cerca/ search bar.	6.1	More Details
CVE-2020-15537	An issue was discovered in the Vanguard plugin 2.1 for WordPress. XSS can occur via the mails/new title field, a product field to the p/ URI, or the Products Search box.	6.1	More Details
CVE-2020-15536	An issue was discovered in the bestsoftinc Hotel Booking System Pro plugin through 1.1 for WordPress. Persistent XSS can occur via any of the registration fields.	6.1	More Details
CVE-2020-15535	An issue was discovered in the bestsoftinc Car Rental System plugin through 1.3 for WordPress. Persistent XSS can occur via any of the registration fields.	6.1	More Details
CVE-2020-3282	A vulnerability in the web-based management interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	6.1	More Details
CVE-2020-14169	The quick search component in Atlassian Jira Server and Data Center before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability	6.1	More Details
CVE-2020-2206	Jenkins VncRecorder Plugin 1.25 and earlier does not escape a parameter value in the checkVncServ form validation endpoint, resulting in a reflected cross-site scripting (XSS) vulnerability.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2207	Jenkins VncViewer Plugin 1.7 and earlier does not escape a parameter value in the checkVncServ form validation endpoint, resulting in a reflected cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2019-19935	Froala Editor before 3.2.3 allows XSS.	6.1	More Details
CVE-2020-11882	The O2 Business application 1.2.0 for Android exposes the canvasm.myo2.SplashActivity activity to other applications. The purpose of this activity is to handle deeplinks that can be delivered either via links or by directly calling the activity. However, the deeplink format is not properly validated. This can be abused by an attacker to redirect a user to any page and deliver any content to the user.	6.1	More Details
CVE-2020-4022	The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a mixed multipart content type.	6.1	More Details
CVE-2017-1659	"HCL iNotes is susceptible to a Cross-Site Scripting (XSS) Vulnerability. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials."	6.1	More Details
CVE-2020-15575	SolarWinds Serv-U File Server before 15.2.1 allows XSS as demonstrated by Tenable Scan, aka Case Number 00484194.	6.1	More Details
CVE-2020-15599	Victor CMS through 2019-02-28 allows XSS via the register.php user_firstname or user_lastname field.	6.1	More Details
CVE-2020-15500	An issue was discovered in server.js in TileServer GL through 3.0.0. The content of the key GET parameter is reflected unsanitized in an HTTP response for the application's main page, causing reflected XSS.	6.1	More Details
CVE-2020-15573	SolarWinds Serv-U File Server before 15.2.1 has a "Cross-script vulnerability," aka Case Numbers 00041778 and 00306421.	6.1	More Details
CVE-2020-14055	Monsta FTP 2.10.1 or below is prone to a stored cross-site scripting vulnerability in the language setting due to insufficient output encoding.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2217	Jenkins Compatibility Action Storage Plugin 1.0 and earlier does not escape the content coming from the MongoDB in the testConnection form validation endpoint, resulting in a reflected cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2019-4324	"HCL AppScan Enterprise is susceptible to Cross-Site Scripting while importing a specially crafted test policy."	6.1	More Details
CVE-2020-14164	The WYSIWYG editor resource in Jira Server and Data Center before version 8.8.2 allows remote attackers to inject arbitrary HTML or JavaScript names via an Cross Site Scripting (XSS) vulnerability by pasting javascript code into the editor field.	6.1	More Details
CVE-2020-8176	A cross-site scripting vulnerability exists in koa-shopify-auth v3.1.61-v3.1.62 that allows an attacker to inject JS payloads into the `shop` parameter on the `/shopify/auth/enable_cookies` endpoint.	6.1	More Details
CVE-2020-7689	Data is truncated wrong when its length is greater than 255 bytes.	5.9	More Details
CVE-2017-1712	"A vulnerability in the TLS protocol implementation of the Domino server could allow an unauthenticated, remote attacker to access sensitive information, aka a Return of Bleichenbacher's Oracle Threat (ROBOT) attack. An attacker could iteratively query a server running a vulnerable TLS stack implementation to perform cryptanalytic operations that may allow decryption of previously captured TLS sessions."	5.9	More Details
CVE-2020-14168	The email client in Jira Server and Data Center before version 7.13.16, from 8.5.0 before 8.5.7, from 8.8.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to access outgoing emails between a Jira instance and the SMTP server via man-in-the-middle (MITM) vulnerability.	5.9	More Details
CVE-2020-15583	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. StickerProvider allows directory traversal for access to system files. The Samsung ID is SVE-2020-17665 (July 2020).	5.5	More Details
CVE-2020-5908	In versions bundled with BIG-IP APM 12.1.0-12.1.5 and 11.6.1-11.6.5.2, Edge Client for Linux exposes full session ID in the local log files.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8252	Adobe Acrobat and Reader versions 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a type confusion vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-15582	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 7885 chipsets) software. The Bluetooth Low Energy (BLE) component has a buffer overflow with a resultant deadlock or crash. The Samsung ID is SVE-2020-16870 (July 2020).	5.5	More Details
CVE-2020-1838	HUAWEI Mate 30 Pro with versions earlier than 10.1.0.150(C00E136R5P3) have is an improper authentication vulnerability. The device does not sufficiently validate certain credential of user's face, an attacker could craft the credential of the user, successful exploit could allow the attacker to pass the authentication with the crafted credential.	5.5	More Details
CVE-2020-15584	An issue was discovered on Samsung mobile devices with Q(10.0) software. Attackers can trigger an out-of-bounds access and device reset via a 4K wallpaper image because ImageProcessHelper mishandles boundary checks. The Samsung ID is SVE-2020-18056 (July 2020).	5.5	More Details
CVE-2020-15577	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Cameralyzer allows attackers to write files to the SD card. The Samsung ID is SVE-2020-16830 (July 2020).	5.5	More Details
CVE-2019-8251	Adobe Acrobat and Reader versions 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a type confusion vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-9226	HUAWEI P30 with versions earlier than 10.1.0.135(C00E135R2P11) have an improper signature verification vulnerability. The system does not improper check signature of specific software package, an attacker may exploit this vulnerability to load a crafted software package to the device.	5.5	More Details
CVE-2020-15570	The parse_report() function in whoopsie.c in Whoopsie through 0.2.69 mishandles memory allocation failures, which allows an attacker to cause a denial of service via a malformed crash file.	5.5	More Details
CVE-2020-15569	PlayerGeneric.cpp in MilkyTracker through 1.02.00 has a use-after-free in the PlayerGeneric destructor.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15578	An issue was discovered on Samsung mobile devices with O(8.x) software. FactoryCamera does not properly restrict runtime permissions. The Samsung ID is SVE-2020-17270 (July 2020).	5.5	More Details
CVE-2020-15470	ffjpeg through 2020-02-24 has a heap-based buffer overflow in jfif_decode in jfif.c.	5.5	More Details
CVE-2020-15580	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Attackers can bypass Factory Reset Protection (FRP) by enrolling a new lock password. The Samsung ID is SVE-2020-17328 (July 2020).	5.5	More Details
CVE-2020-4024	The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a vnd.wap.xhtml+xml content type.	5.4	More Details
CVE-2020-15517	The ke_search (aka Faceted Search) extension through 2.8.2, and 3.x through 3.1.3, for TYPO3 allows XSS.	5.4	More Details
CVE-2020-15516	The mm_forum extension through 1.9.5 for TYPO3 allows XSS that can be exploited via CSRF.	5.4	More Details
CVE-2020-15514	The jh_captcha extension through 2.1.3, and 3.x through 3.0.2, for TYPO3 allows XSS.	5.4	More Details
CVE-2020-15036	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Topology-Linked.php dv parameter.	5.4	More Details
CVE-2020-15031	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Assets-Management.php chg parameter.	5.4	More Details
CVE-2020-2214	Jenkins ZAP Pipeline Plugin 1.9 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download.	5.4	More Details
CVE-2020-15034	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Monitoring-Setup.php tet parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15033	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the snmpget.php ip parameter.	5.4	More Details
CVE-2020-15032	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Monitoring-Incidents.php id parameter.	5.4	More Details
CVE-2020-11074	In PrestaShop from version 1.5.3.0 and before version 1.7.6.6, there is a stored XSS when using the name of a quick access item. The problem is fixed in 1.7.6.6.	5.4	More Details
CVE-2020-14173	The file upload feature in Atlassian Jira Server and Data Center in affected versions allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability. The affected versions are before version 8.5.4, from version 8.6.0 before 8.6.2, and from version 8.7.0 before 8.7.1.	5.4	More Details
CVE-2020-5909	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, when users run the command displayed in NGINX Controller user interface (UI) to fetch the agent installer, the server TLS certificate is not verified.	5.4	More Details
CVE-2020-15030	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Topology-Routes.php rtr parameter.	5.4	More Details
CVE-2020-2219	Jenkins Link Column Plugin 1.0 and earlier does not filter URLs of links created by users with View/Configure permission, resulting in a stored cross-site scripting vulnerability.	5.4	More Details
CVE-2020-15029	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Assets-Management.php sn parameter.	5.4	More Details
CVE-2020-15028	NeDi 1.9C is vulnerable to a cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Topology-Map.php xo parameter.	5.4	More Details
CVE-2020-15037	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Reports-Devices.php page st[] parameter.	5.4	More Details
CVE-2020-2204	A missing permission check in Jenkins Fortify on Demand Plugin 5.0.1 and earlier allows attackers with Overall/Read permission to connect to the globally configured Fortify on Demand endpoint using attacker-specified credentials IDs.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2201	Jenkins Sonargraph Integration Plugin 3.0.0 and earlier does not escape the file path for the Log file field form validation, resulting in a stored cross-site scripting vulnerability.	5.4	More Details
CVE-2020-15035	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Monitoring-Map.php hde parameter.	5.4	More Details
CVE-2020-14165	The UniversalAvatarResource.getAvatars resource in Jira Server and Data Center before version 8.9.0 allows remote attackers to obtain information about custom project avatars names via an Improper authorization vulnerability.	5.3	More Details
CVE-2020-15581	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The kernel logging feature allows attackers to discover virtual addresses via vectors involving shared memory. The Samsung ID is SVE-2020-17605 (July 2020).	5.3	More Details
CVE-2020-15525	GitLab EE 11.3 through 13.1.2 has Incorrect Access Control because of the Maven package upload endpoint.	5.3	More Details
CVE-2020-15392	A user enumeration vulnerability flaw was found in Venki Supravizio BPM 10.1.2. This issue occurs during password recovery, where a difference in error messages could allow an attacker to determine if a username is valid or not, enabling a brute-force attack with valid usernames.	5.3	More Details
CVE-2020-15513	The typo3_forum extension before 1.2.1 for TYPO3 has Incorrect Access Control.	5.3	More Details
CVE-2020-15081	In PrestaShop from version 1.5.0.0 and before 1.7.6.6, there is information exposure in the upload directory. The problem is fixed in version 1.7.6.6. A possible workaround is to add an empty index.php file in the upload directory.	5.3	More Details
CVE-2019-20408	The /plugins/servlet/gadgets/makeRequest resource in Jira before version 8.7.0 allows remote attackers to access the content of internal network resources via a Server Side Request Forgery (SSRF) vulnerability due to a logic bug in the JiraWhitelist class.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1836	HUAWEI P30 with versions earlier than 10.1.0.160(C00E160R2P11) and HUAWEI P30 Pro with versions earlier than 10.1.0.160(C00E160R2P8) have an information disclosure vulnerability. Certain function's default configuration in the system seems insecure, an attacker should craft a WI-FI hotspot to launch the attack. Successful exploit could cause information disclosure.	5.3	More Details
CVE-2020-6261	SAP Solution Manager (Trace Analysis), version 7.20, allows an attacker to perform a log injection into the trace file, due to Incomplete XML Validation. The readability of the trace file is impaired.	5.3	More Details
CVE-2020-4355	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a denial of service, caused by improper handling of Secure Sockets Layer (SSL) renegotiation requests. By sending specially-crafted requests, a remote attacker could exploit this vulnerability to increase the resource usage on the system. IBM X-Force ID: 178507.	5.3	More Details
CVE-2020-1837	ChangXiang 8 Plus with versions earlier than 9.1.0.136(C00E121R1P6T8) have a denial of service vulnerability. The device does not properly handle certain message from base station, the attacker could craft a fake base station to launch the attack. Successful exploit could cause a denial of signal service condition.	5.3	More Details
CVE-2020-14196	In PowerDNS Recursor versions up to and including 4.3.1, 4.2.2 and 4.1.16, the ACL restricting access to the internal web server is not properly enforced.	5.3	More Details
CVE-2020-15080	In PrestaShop from version 1.7.4.0 and before version 1.7.6.6, some files should not be in the release archive, and others should not be accessible. The problem is fixed in version 1.7.6.6 A possible workaround is to make sure `composer.json` and `docker-compose.yml` are not accessible on your server.	5.3	More Details
CVE-2020-8916	A memory leak in Openthread's wpantund versions up to commit 0e5d1601febb869f583e944785e5685c6c747be7, when used in an environment where wpanctl is directly interfacing with the control driver (eg: debug environments) can allow an attacker to crash the service (DoS). We recommend updating, or to restrict access in your debug environments.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14166	The /servicedesk/customer/portals resource in Jira Service Desk Server and Data Center before version 4.10.0 allows remote attackers with project administrator privileges to inject arbitrary HTML or JavaScript names via an Cross Site Scripting (XSS) vulnerability by uploading a html file.	4.8	More Details
CVE-2020-2205	Jenkins VncRecorder Plugin 1.25 and earlier does not escape a tool path in the `checkVncServ` form validation endpoint, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by Jenkins administrators.	4.8	More Details
CVE-2020-4025	The attachment download resource in Atlassian Jira Server and Data Center The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a rdf content type.	4.8	More Details
CVE-2020-3340	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input that is processed by the web-based management interface. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need valid administrative credentials.	4.8	More Details
CVE-2020-15083	In PrestaShop from version 1.7.0.0 and before version 1.7.6.6, if a target sends a corrupted file, it leads to a reflected XSS. The problem is fixed in 1.7.6.6	4.7	More Details
CVE-2020-4027	Affected versions of Atlassian Confluence Server and Data Center allowed remote attackers with system administration permissions to bypass velocity template injection mitigations via an injection vulnerability in custom user macros. The affected versions are before version 7.4.5, and from version 7.5.0 before 7.5.1.	4.7	More Details
CVE-2020-4387	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to obtain sensitive information using a race condition of a symbolic link. IBM X-Force ID: 179269.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4386	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to obtain sensitive information using a race condition of a symbolic link. IBM X-Force ID: 179268.	4.7	More Details
CVE-2020-4414	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local attacker to perform unauthorized actions on the system, caused by improper usage of shared memory. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information or cause a denial of service. IBM X-Force ID: 179989.	4.4	More Details
CVE-2020-9497	Apache Guacamole 1.1.0 and older do not properly validate datareceived from RDP servers via static virtual channels. If a userconnects to a malicious or compromised RDP server, specially-craftedPDUs could result in disclosure of information within the memory ofthe guacd process handling the connection.	4.4	More Details
CVE-2020-15095	Versions of the npm CLI prior to 6.14.6 are vulnerable to an information exposure vulnerability through log files. The CLI supports URLs like "<protocol>://[<user>[:<password>]@]<hostname>[:<port>][:][/]<path>". The password value is not redacted and is printed to stdout and also to any generated log files.	4.4	More Details
CVE-2020-5905	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display.	4.3	More Details
CVE-2020-2212	Jenkins GitHub Coverage Reporter Plugin 1.8 and earlier stores secrets unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system or read permissions on the system configuration.	4.3	More Details
CVE-2020-4029	The /rest/project-templates/1.0/createshared resource in Atlassian Jira Server and Data Center before version 8.5.5, from 8.6.0 before 8.7.2, and from 8.8.0 before 8.8.1 allows remote attackers to enumerate project names via an improper authorization vulnerability.	4.3	More Details
CVE-2019-4704	IBM Security Identity Manager Virtual Appliance 7.0.2 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: 172014.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8166	A CSRF forgery vulnerability exists in rails < 5.2.5, rails < 6.0.4 that makes it possible for an attacker to, given a global CSRF token such as the one present in the authenticity_token meta tag, forge a per-form CSRF token.	4.3	More Details
CVE-2020-2216	A missing permission check in Jenkins Zephyr for JIRA Test Management Plugin 1.5 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified username and password.	4.3	More Details
CVE-2020-2215	A cross-site request forgery vulnerability in Jenkins Zephyr for JIRA Test Management Plugin 1.5 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified username and password.	4.3	More Details
CVE-2020-2213	Jenkins White Source Plugin 19.1.1 and earlier stores credentials unencrypted in its global configuration file and in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission (config.xml), or access to the master file system.	4.3	More Details
CVE-2020-2210	Jenkins Stash Branch Parameter Plugin 0.3.0 and earlier transmits configured passwords in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.	4.3	More Details
CVE-2020-2209	Jenkins TestComplete support Plugin 2.4.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	4.3	More Details
CVE-2020-2208	Jenkins Slack Upload Plugin 1.7 and earlier stores a secret unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	4.3	More Details
CVE-2020-2203	A cross-site request forgery vulnerability in Jenkins Fortify on Demand Plugin 5.0.1 and earlier allows attackers to connect to the globally configured Fortify on Demand endpoint using attacker-specified credentials IDs.	4.3	More Details
CVE-2019-4323	"HCL AppScan Enterprise advisory API documentation is susceptible to clickjacking, which could allow an attacker to embed the contents of untrusted web pages in a frame."	4.3	More Details
CVE-2020-2202	A missing permission check in Jenkins Fortify on Demand Plugin 6.0.0 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8179	Improper access control in Nextcloud Deck 1.0.0 allowed an attacker to inject tasks into other users decks.	4.1	More Details
CVE-2020-4061	In October from version 1.0.319 and before version 1.0.467, pasting content copied from malicious websites into the Froala richeditor could result in a successful self-XSS attack. This has been fixed in 1.0.467.	3.7	More Details
CVE-2020-2218	Jenkins HP ALM Quality Center Plugin 1.6 and earlier stores a password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	3.3	More Details
CVE-2019-4706	IBM Security Identity Manager Virtual Appliance 7.0.2 writes information to log files which can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information. IBM X-Force ID: 172016.	2.7	More Details
CVE-2019-4705	IBM Security Identity Manager Virtual Appliance 7.0.2 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 172015.	2.7	More Details
CVE-2020-15469	In QEMU 4.2.0, a MemoryRegionOps object may lack read/write callback methods, leading to a NULL pointer dereference.	2.3	More Details
CVE-2019-20417	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-15011. Reason: This candidate is a reservation duplicate of CVE-2019-15011. Notes: All CVE users should reference CVE-2019-15011 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details