SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 05 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-2020-10731 | A flaw was found in the nova_libvirt container provided by the Red Hat OpenStack Platform 16, where it does not have SELinux enabled. This flaw causes sVirt, an important isolation mechanism, to be disabled for all running virtual machines. | 9.9 | More Details |
| CVE-2020-3374 | A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization, enabling them to access sensitive information, modify the system configuration, or impact the availability of the affected system. The vulnerability is due to insufficient authorization checking on the affected system. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to gain privileges beyond what would normally be authorized for their configured user authorization level. The attacker may be able to access sensitive information, modify the system configuration, or impact the availability of the affected system. | 9.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-14316 | A flaw was found in kubevirt 0.29 and earlier. Virtual Machine Instances (VMIs) can be used to gain access to the host's filesystem. Successful exploitation allows an attacker to assume the privileges of the VM process on the host system. In worst-case scenarios an attacker can read and modify any file on the system where the VMI is running. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. | 9.9 | More Details |
| CVE-2020-7697 | This affects all versions of package mock2easy. a malicious user could inject commands through the _data variable: Affected Area require('../server/getJsonByCurl')(mock2easy, function (error, stdout) { if (error) { return res.json(500, error); } res.json(JSON.parse(stdout)); }, '', _data.interfaceUrl, query, _data.cookie,_data.interfaceType); | 9.8 | More Details |
| CVE-2020-3688 | Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 | 9.8 | More Details |
| CVE-2020-5616 | [Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01], [CalendarForm01], and [Link01] [Calendar01] free edition ver1.0.0, [Calendar02] free edition ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01] free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0, [Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0 allows remote attackers to bypass authentication and log in to the product with administrative privileges via unspecified vectors. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-5413 | Spring Integration framework provides Kryo Codec implementations as an alternative for Java (de)serialization. When Kryo is configured with default options, all unregistered classes are resolved on demand. This leads to the "deserialization gadgets" exploit when provided data contains malicious code for execution during deserialization. In order to protect against this type of attack, Kryo can be configured to require a set of trusted classes for (de)serialization. Spring Integration should be proactive against blocking unknown "deserialization gadgets" when configuring Kryo in code. | 9.8 | More Details |
| CVE-2020-3681 | Authenticated and encrypted payload MMEs can be forged and remotely sent to any HPAV2 system using a jailbreak key recoverable from code. | 9.8 | More Details |
| CVE-2020-3382 | A vulnerability in the REST API of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device. The vulnerability exists because different installations share a static encryption key. An attacker could exploit this vulnerability by using the static key to craft a valid session token. A successful exploit could allow the attacker to perform arbitrary actions through the REST API with administrative privileges. | 9.8 | More Details |
| CVE-2020-3375 | A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access, make changes to the system that they are not authorized to make, and execute commands on an affected system with privileges of the root user. | 9.8 | More Details |
| CVE-2020-16165 | The DAO/DTO implementation in SpringBlade through 2.7.1 allows SQL Injection in an ORDER BY clause. This is related to the /api/blade-log/api/list ascs and desc parameters. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-3698 | Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 | 9.8 | More Details |
| CVE-2020-3699 | Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 | 9.8 | More Details |
| CVE-2020-3671 | Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 | 9.8 | More Details |
| CVE-2019-20027 | Aspire-derived NEC PBXes, including the SV8100, SV9100, SL1100 and SL2100 with software releases 7.0 or higher contain the possibility if incorrectly configured to allow a blank username and password combination to be entered as a valid, successfully authenticating account. | 9.8 | More Details |
| CVE-2020-2076 | SICK Package Analytics software up to and including version V04.0.0 are vulnerable to an authentication bypass by directly interfacing with the REST API. An attacker can send unauthorized requests, bypass current authentication controls presented by the application and could potentially write files without authentication. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-4567 | IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 184156. | 9.8 | More Details |
| CVE-2020-15588 | An issue was discovered in the client side of Zoho ManageEngine Desktop Central 10.0.552.W. An attacker-controlled server can trigger an integer overflow in InternetSendRequestEx and InternetSendRequestByBitrate that leads to a heap-based buffer overflow and Remote Code Execution with SYSTEM privileges. This issue will occur only when untrusted communication is initiated with server. In cloud, Agent will always connect with trusted communication. | 9.8 | More Details |
| CVE-2019-20025 | Certain builds of NEC SV9100 software could allow an unauthenticated, remote attacker to log into a device running an affected release with a hardcoded username and password, aka a Static Credential Vulnerability. The vulnerability is due to an undocumented user account with manufacturer privilege level. An attacker could exploit this vulnerability by using this account to remotely log into an affected device. A successful exploit could allow the attacker to log into the device with manufacturer level access. This vulnerability affects SV9100 PBXes that are running software release 6.0 or higher. This vulnerability does not affect SV9100 software releases prior to 6.0. | 9.8 | More Details |
| CVE-2020-15086 | In TYPO3 installations with the "mediace" extension from version 7.6.2 and before version 7.6.5, it has been discovered that an internal verification mechanism can be used to generate arbitrary checksums. The allows to inject arbitrary data having a valid cryptographic message authentication code and can lead to remote code execution. To successfully exploit this vulnerability, an attacker must have access to at least one `Extbase` plugin or module action in a TYPO3 installation. This is fixed in version 7.6.5 of the "mediace" extension for TYPO3. | 9.8 | More Details |
| CVE-2019-20033 | On Aspire-derived NEC PBXes, including all versions of SV8100 devices, a set of documented, static login credentials may be used to access the DIM interface. | 9.8 | More Details |
| CVE-2020-4459 | IBM Security Verify Access 10.7 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 181395. | 9.8 | More Details |
| CVE-2020-9691 | Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have a dom-based cross-site scripting vulnerability. Successful exploitation could lead to arbitrary code execution. | 9.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-14487 | OpenClinic GA 5.09.02 contains a hidden default user account that may be accessed if an administrator has not expressly turned off this account, which may allow an attacker to login and execute arbitrary commands. | 9.4 | More Details |
| CVE-2019-20031 | NEC UM8000, UM4730 and prior non-InMail voicemail systems with all known software versions may permit an infinite number of login attempts in the telephone user interface (TUI), effectively allowing brute force attacks. | 9.1 | More Details |
| CVE-2020-16163 | An issue was discovered in RIPE NCC RPKI Validator 3.x before 3.1-2020.07.06.14.28. RRDP fetches proceed even with a lack of validation of a TLS HTTPS endpoint. This allows remote attackers to bypass intended access restrictions, or to trigger denial of service to traffic directed to co-dependent routing systems. NOTE: third parties assert that the behavior is intentionally permitted by RFC 8182 | 9.1 | More Details |
| CVE-2020-14158 | The ABUS Secvest FUMO50110 hybrid module does not have any security mechanism that ensures confidentiality or integrity of RF packets that are exchanged with an alarm panel. This makes it easier to conduct wAppLoxx authentication-bypass attacks. | 9.1 | More Details |
| CVE-2019-11286 | VMware GemFire versions prior to 9.10.0, 9.9.1, 9.8.5, and 9.7.5, and VMware Tanzu GemFire for VMs versions prior to 1.11.0, 1.10.1, 1.9.2, and 1.8.2, contain a JMX service available to the network which does not properly restrict input. A remote authenticated malicious user may request against the service with a crafted set of credentials leading to remote code execution. | 9.1 | More Details |
| CVE-2020-4377 | IBM Cognos Anaytics 11.0 and 11.1 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: 179156. | 9.1 | More Details |
| CVE-2020-16271 | The SRP-6a implementation in Kee Vault KeePassRPC before 1.12.0 generates insufficiently random numbers, which allows remote attackers to read and modify data in the KeePass database via a WebSocket connection. | 9.1 | More Details |
| CVE-2020-16272 | The SRP-6a implementation in Kee Vault KeePassRPC before 1.12.0 is missing validation for a client-provided parameter, which allows remote attackers to read and modify data in the KeePass database via an A=0 WebSocket connection. | 9.1 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-5763 | Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. | 8.8 | More Details |
| CVE-2020-14488 | OpenClinic GA 5.09.02 and 5.89.05b does not properly verify uploaded files, which may allow a low-privilege user to upload and execute arbitrary files on the system. | 8.8 | More Details |
| CVE-2020-3386 | A vulnerability in the REST API endpoint of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker with a low-privileged account to bypass authorization on the API of an affected device. The vulnerability is due to insufficient authorization of certain API functions. An attacker could exploit this vulnerability by sending a crafted request to the API using low-privileged credentials. A successful exploit could allow the attacker to perform arbitrary actions through the REST API with administrative privileges. | 8.8 | More Details |
| CVE-2020-5773 | Improper Access Control in Teltonika firmware TRB2_R_00.02.04.01 allows a low privileged user to perform unauthorized write operations. | 8.8 | More Details |
| CVE-2020-15871 | Sonatype Nexus Repository Manager OSS/Pro version before 3.25.1 allows Remote Code Execution. | 8.8 | More Details |
| CVE-2020-5396 | VMware GemFire versions prior to 9.10.0, 9.9.2, 9.8.7, and 9.7.6, and VMware Tanzu GemFire for VMs versions prior to 1.11.1 and 1.10.2, when deployed without a SecurityManager, contain a JMX service available which contains an insecure default configuration. This allows a malicious user to create an MLet mbean leading to remote code execution. | 8.8 | More Details |
| CVE-2020-15467 | The administrative interface of Cohesive Networks vns3:vpn appliances before version 4.11.1 is vulnerable to authenticated remote code execution leading to server compromise. | 8.8 | More Details |
| CVE-2019-20029 | An exploitable privilege escalation vulnerability exists in the WebPro functionality of Aspire-derived NEC PBXes, including all versions of SV8100, SV9100, SL1100 and SL2100 devices. A specially crafted HTTP POST can cause privilege escalation resulting in a higher privileged account, including an undocumented developer level of access. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-15098 | In TYPO3 CMS greater than or equal to 9.0.0 and less than 9.5.20, and greater than or equal to 10.0.0 and less than 10.4.6, it has been discovered that an internal verification mechanism can be used to generate arbitrary checksums. This allows to inject arbitrary data having a valid cryptographic message authentication code (HMAC-SHA1) and can lead to various attack chains including potential privilege escalation, insecure deserialization & remote code execution. The overall severity of this vulnerability is high based on mentioned attack chains and the requirement of having a valid backend user session (authenticated). This has been patched in versions 9.5.20 and 10.4.6. | 8.8 | More Details |
| CVE-2020-13699 | TeamViewer Desktop for Windows before 15.8.3 does not properly quote its custom URI handlers. A malicious website could launch TeamViewer with arbitrary parameters, as demonstrated by a teamviewer10: --play URL. An attacker could force a victim to send an NTLM authentication request and either relay the request or capture the hash for offline password cracking. This affects teamviewer10, teamviewer8, teamviewerapi, tvchat1, tvcontrol1, tvfiletransfer1, tvjoinv8, tvpresent1, tvsendfile1, tvsqcustomer1, tvsqsupport1, tvvideocall1, and tvvpn1. The issue is fixed in 8.0.258861, 9.0.258860, 10.0.258873, 11.0.258870, 12.0.258869, 13.2.36220, 14.2.56676, 14.7.48350, and 15.8.3. | 8.8 | More Details |
| CVE-2020-4534 | IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a local authenticated attacker to gain elevated privileges on the system, caused by improper handling of UNC paths. By scheduling a task with a specially-crafted UNC path, an attacker could exploit this vulnerability to execute arbitrary code with higher privileges. IBM X-Force ID: 182808. | 8.8 | More Details |
| CVE-2020-14334 | A flaw was found in Red Hat Satellite 6 which allows privileged attacker to read cache files. These cache credentials could help attacker to gain complete control of the Satellite instance. | 8.8 | More Details |
| CVE-2020-3383 | A vulnerability in the archive utility of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. The vulnerability is due to a lack of proper input validation of paths that are embedded within archive files. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit could allow the attacker to write arbitrary files in the system with the privileges of the logged-in user. | 8.8 | More Details |
| CVE-2020-5615 | Cross-site request forgery (CSRF) vulnerability in [Calendar01] free edition ver1.0.0 and [Calendar02] free edition ver1.0.0 allows remote attackers to hijack the authentication of administrators via unspecified vectors. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-5770 | Cross-site request forgery in Teltonika firmware TRB2_R_00.02.04.01 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link. | 8.8 | More Details |
| CVE-2020-14493 | A low-privilege user may use SQL syntax to write arbitrary files to the OpenClinic GA 5.09.02 and 5.89.05b server, which may allow the execution of arbitrary commands. | 8.8 | More Details |
| CVE-2020-14490 | OpenClinic GA 5.09.02 and 5.89.05b includes arbitrary local files specified within its parameter and executes some files, which may allow disclosure of sensitive files or the execution of malicious uploaded files. | 8.8 | More Details |
| CVE-2020-5384 | Authentication Bypass Vulnerability RSA MFA Agent 2.0 for Microsoft Windows contains an Authentication Bypass vulnerability. A local unauthenticated attacker could potentially exploit this vulnerability by using an alternate path to bypass authentication in order to gain full access to the system. | 8.4 | More Details |
| CVE-2020-3384 | A vulnerability in specific REST API endpoints of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to inject arbitrary commands on the underlying operating system with the privileges of the logged-in user. The vulnerability is due to insufficient validation of user-supplied input to the API. An attacker could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to inject arbitrary commands on the underlying operating system. | 8.2 | More Details |
| CVE-2020-10713 | A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. | 8.2 | More Details |
| CVE-2020-8108 | Improper Authentication vulnerability in Bitdefender Endpoint Security for Mac allows an unprivileged process to restart the main service and potentially inject third-party code into a trusted process. This issue affects: Bitdefender Endpoint Security for Mac versions prior to 4.12.80. | 8.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-4463 | IBM Maximo Asset Management 7.6.0.1 and 7.6.0.2 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: 181484. | 8.2 | More Details |
| CVE-2020-15943 | An issue was discovered in the Gantt-Chart module before 5.5.4 for Jira. Due to a missing privilege check, it is possible to read and write to the module configuration of other users. This can also be used to deliver an XSS payload to other users' dashboards. To exploit this vulnerability, an attacker has to be authenticated. | 8.1 | More Details |
| CVE-2020-8206 | An improper authentication vulnerability exists in Pulse Connect Secure <9.1RB that allows an attacker with a users primary credentials to bypass the Google TOTP. | 8.1 | More Details |
| CVE-2020-15099 | In TYPO3 CMS greater than or equal to 9.0.0 and less than 9.5.20, and greater than or equal to 10.0.0 and less than 10.4.6, in a case where an attacker manages to generate a valid cryptographic message authentication code (HMAC-SHA1) - either by using a different existing vulnerability or in case the internal encryptionKey was exposed - it is possible to retrieve arbitrary files of a TYPO3 installation. This includes the possibility to fetch typo3conf/LocalConfiguration.php, which again contains the encryptionKey as well as credentials of the database management system being used. In case a database server is directly accessible either via internet or in a shared hosting network, this allows the ability to completely retrieve, manipulate or delete database contents. This includes creating an administration user account - which can be used to trigger remote code execution by injecting custom extensions. This has been patched in versions 9.5.20 and 10.4.6. | 8.1 | More Details |
| CVE-2020-7698 | This affects the package Gerapy from 0 and before 0.9.3. The input being passed to Popen, via the project_configure endpoint, isn’t being sanitized. | 8.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-15133 | In faye-websocket before version 0.11.0, there is a lack of certification validation in TLS handshakes. The `Faye::WebSocket::Client` class uses the `EM::Connection#start_tls` method in EventMachine to implement the TLS handshake whenever a `wss:` URL is used for the connection. This method does not implement certificate verification by default, meaning that it does not check that the server presents a valid and trusted TLS certificate for the expected hostname. That means that any `wss:` connection made using this library is vulnerable to a man-in-the-middle attack, since it does not confirm the identity of the server it is connected to. For further background information on this issue, please see the referenced GitHub Advisory. Upgrading `faye-websocket` to v0.11.0 is recommended. | 8.0 | More Details |
| CVE-2020-16134 | An issue was discovered on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to 10.04.38, Internet Box 3 prior to 11.01.20, and Internet Box light prior to 08.06.06. Given the (user-configurable) credentials for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the superuser. | 8.0 | More Details |
| CVE-2020-15134 | Faye before version 1.4.0, there is a lack of certification validation in TLS handshakes. Faye uses em-http-request and faye-websocket in the Ruby version of its client. Those libraries both use the `EM::Connection#start_tls` method in EventMachine to implement the TLS handshake whenever a `wss:` URL is used for the connection. This method does not implement certificate verification by default, meaning that it does not check that the server presents a valid and trusted TLS certificate for the expected hostname. That means that any `https:` or `wss:` connection made using these libraries is vulnerable to a man-in-the-middle attack, since it does not confirm the identity of the server it is connected to. The first request a Faye client makes is always sent via normal HTTP, but later messages may be sent via WebSocket. Therefore it is vulnerable to the same problem that these underlying libraries are, and we needed both libraries to support TLS verification before Faye could claim to do the same. Your client would still be insecure if its initial HTTPS request was verified, but later WebSocket connections were not. This is fixed in Faye v1.4.0, which enables verification by default. For further background information on this issue, please see the referenced GitHub Advisory. | 8.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-16203 | Delta Industrial Automation CNCSoft ScreenEditor, Versions 1.01.23 and prior. An uninitialized pointer 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-2020-16143 | The seafile-client client 7.0.8 for Seafile is vulnerable to DLL hijacking because it loads exchndl.dll from the current working directory. | 7.8 | More Details |
| CVE-2020-3701 | Use after free issue while processing error notification from camx driver due to not properly releasing the sequence data in Snapdragon Mobile in Saipan, SM8250, SXR2130 | 7.8 | More Details |
| CVE-2020-5610 | Global TechStream (GTS) for TOYOTA dealers version 15.10.032 and earlier allows an attacker to cause a denial-of-service (DoS) condition and execute arbitrary code via unspecified vectors. | 7.8 | More Details |
| CVE-2020-7822 | DaviewIndy has a Heap-based overflow vulnerability, triggered when the user opens a malformed image file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. | 7.8 | More Details |
| CVE-2019-14130 | Memory corruption can occurs in trusted application if offset size from HLOS is more than actual mapped buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 | 7.8 | More Details |
| CVE-2019-10580 | When kernel thread unregistered listener, Use after free issue happened as the listener client`s private data has been already freed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MSM8909W, Nicobar, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDM429W, SDX55, SM8150, SM8250, SXR2130 | 7.8 | More Details |
| CVE-2019-14037 | Close and bind operations done on a socket can lead to a Use-After-Free condition. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8996, MSM8996AU, QCN7605, QCN7606, QCS605, SC8180X, SDA660, SDA845, SDM439, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2019-14093 | Array out of bound access can occur in display module due to lack of bound check on input parcel received in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCM2150, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM636, SDM660, SDX20 | 7.8 | More Details |
| CVE-2019-14100 | Register write via debugfs is disabled by default to prevent register writing via debugfs. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9206, MDM9207C, MDM9607, Nicobar, QCS405, SA6155P, SC8180X, SDX55, SM8150 | 7.8 | More Details |
| CVE-2019-14123 | Possible buffer overflow and over read possible due to missing bounds checks for fixed limits if we consider widevine HLOS client as non-trustable in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 | 7.8 | More Details |
| CVE-2019-14124 | Memory failure in content protection module due to not having pointer within the scope in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130 | 7.8 | More Details |
| CVE-2019-14099 | Device misbehavior may be observed when incorrect offset, length or number of buffers is passed by user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 | 7.8 | More Details |
| CVE-2019-20030 | An attacker with knowledge of the modem access number on a NEC UM8000 voicemail system may use SSH tunneling or standard Linux utilities to gain access to the system's LAN port. All versions are affected. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-5760 | Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. | 7.8 | More Details |
| CVE-2020-7828 | DaviewIndy 8.98.4 and earlier version contain Heap-based overflow vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. | 7.8 | More Details |
| CVE-2020-8574 | Active IQ Unified Manager for Linux versions prior to 9.6 ship with the Java Management Extension Remote Method Invocation (JMX RMI) service enabled allowing unauthorized code execution to local users. | 7.8 | More Details |
| CVE-2019-19455 | Wowza Streaming Engine before 4.8.5 has Insecure Permissions which may allow a local attacker to escalate privileges in / usr / local / WowzaStreamingEngine / manager / bin / in the Linux version of the server by writing arbitrary commands in any file and execute them as root. This issue was resolved in Wowza Streaming Engine 4.8.5. | 7.8 | More Details |
| CVE-2020-5617 | Privilege escalation vulnerability in SKYSEA Client View Ver.12.200.12n to 15.210.05f allows an attacker to obtain unauthorized privileges and modify/obtain sensitive information or perform unintended operations via unspecified vectors. | 7.8 | More Details |
| CVE-2020-4554 | IBM i2 Analyst Notebook 9.2.1 and 9.2.2 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183322. | 7.8 | More Details |
| CVE-2020-4553 | IBM i2 Analyst Notebook 9.2.1 and 9.2.2 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183321. | 7.8 | More Details |
| CVE-2020-4552 | IBM i2 Analyst Notebook 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183320. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-7829 | DaviewIndy 8.98.4 and earlier version contain Heap-based overflow vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. | 7.8 | More Details |
| CVE-2020-12620 | Pi-hole 4.4 allows a user able to write to /etc/pihole/dns-servers.conf to escalate privileges through command injection (shell metacharacters after an IP address). | 7.8 | More Details |
| CVE-2020-4551 | IBM i2 Analyst Notebook 9.2.1 and 9.2.2 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183319. | 7.8 | More Details |
| CVE-2020-4550 | IBM i2 Analyst Notebook 9.2.1 and 9.2.2 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183318. | 7.8 | More Details |
| CVE-2020-4549 | IBM i2 Analyst Notebook 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183317. | 7.8 | More Details |
| CVE-2020-7827 | DaviewIndy 8.98.7 and earlier version contain Use-After-Free vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. | 7.8 | More Details |
| CVE-2019-20001 | An issue was discovered in RICOH Streamline NX Client Tool and RICOH Streamline NX PC Client that allows attackers to escalate local privileges. | 7.8 | More Details |
| CVE-2020-7823 | DaviewIndy has a Memory corruption vulnerability, triggered when the user opens a malformed image file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. | 7.8 | More Details |
| CVE-2020-14162 | An issue was discovered in Pi-Hole through 5.0. The local www-data user has sudo privileges to execute the pihole core script as root without a password, which could allow an attacker to obtain root access via shell metacharacters to this script's setdns command. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-16199 | Delta Industrial Automation CNCSoft ScreenEditor, Versions 1.01.23 and prior. Multiple stack-based buffer overflow vulnerabilities may be exploited by processing specially crafted project files, which may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application. | 7.8 | More Details |
| CVE-2020-15125 | In auth0 (npm package) versions before 2.27.1, a DenyList of specific keys that should be sanitized from the request object contained in the error object is used. The key for Authorization header is not sanitized and in certain cases the Authorization header value can be logged exposing a bearer token. You are affected by this vulnerability if you are using the auth0 npm package, and you are using a Machine to Machine application authorized to use Auth0's management API | 7.7 | More Details |
| CVE-2020-16136 | In tgstation-server 4.4.0 and 4.4.1, an authenticated user with permission to download logs can download any file on the server machine (accessible by the owner of the server process) via directory traversal ../ sequences in /Administration/Logs/ requests. The attacker is unable to enumerate files, however. | 7.7 | More Details |
| CVE-2020-15130 | In SLPJS (npm package slpjs) before version 0.27.4, there is a vulnerability to false-positive validation outcomes for the NFT1 Child Genesis transaction type. A poorly implemented SLP wallet or opportunistic attacker could create a seemingly valid NFT1 child token without burning any of the NFT1 Group token type as is required by the NFT1 specification. This is fixed in version 0.27.4. | 7.5 | More Details |
| CVE-2020-15957 | An issue was discovered in DP3T-Backend-SDK before 1.1.1 for Decentralised Privacy-Preserving Proximity Tracing (DP3T). When it is configured to check JWT before uploading/publishing keys, it is possible to skip the signature check by providing a JWT token with alg=none. | 7.5 | More Details |
| CVE-2020-14520 | The affected product is vulnerable to an information leak, which may allow an attacker to obtain sensitive information on the Ignition 8 (all versions prior to 8.0.13). | 7.5 | More Details |
| CVE-2020-15131 | In SLP Validate (npm package slp-validate) before version 1.2.2, there is a vulnerability to false-positive validation outcomes for the NFT1 Child Genesis transaction type. A poorly implemented SLP wallet or opportunistic attacker could create a seemingly valid NFT1 child token without burning any of the NFT1 Group token type as is required by the NFT1 specification. This is fixed in version 1.2.2. | 7.5 | More Details |
| CVE-2020-5772 | Improper Input Validation in Teltonika firmware TRB2_R_00.02.04.01 allows a remote, authenticated attacker to gain root privileges by uploading a malicious package file. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-4185 | IBM Security Guardium 10.5, 10.6, and 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174803. | 7.5 | More Details |
| CVE-2020-12081 | An information disclosure vulnerability has been identified in FlexNet Publisher lmadmin.exe 11.14.0.2. The web portal link can be used to access to system files or other important files on the system. | 7.5 | More Details |
| CVE-2020-5771 | Improper Input Validation in Teltonika firmware TRB2_R_00.02.04.01 allows a remote, authenticated attacker to gain root privileges by uploading a malicious backup archive. | 7.5 | More Details |
| CVE-2020-2077 | SICK Package Analytics software up to and including version V04.0.0 are vulnerable due to incorrect default permissions settings. An unauthorized attacker could read sensitive data from the system by querying for known files using the REST API directly. | 7.5 | More Details |
| CVE-2020-15956 | ActiveMediaServer.exe in ACTi NVR3 Standard Server 3.0.12.42 allows remote unauthenticated attackers to trigger a buffer overflow and application termination via a malformed payload. | 7.5 | More Details |
| CVE-2020-4574 | IBM Tivoli Key Lifecycle Manager does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 184181. | 7.5 | More Details |
| CVE-2019-20026 | The WebPro interface in NEC SV9100 software releases 7.0 or higher allows unauthenticated remote attackers to reset all existing usernames and passwords to default values via a crafted request. | 7.5 | More Details |
| CVE-2019-20028 | Aspire-derived NEC PBXes operating InMail software, including all versions of SV8100, SV9100, SL1100 and SL2100 devices allow unauthenticated read-only access to voicemails, greetings, and voice response system content through a system's WebPro administration interface. | 7.5 | More Details |
| CVE-2020-16118 | In GNOME Balsa before 2.6.0, a malicious server operator or man in the middle can trigger a NULL pointer dereference and client crash by sending a PREAUTH response to imap_mbox_connect in libbalsa/imap/imap-handle.c. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-5761 | Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. | 7.5 | More Details |
| CVE-2020-5762 | Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. | 7.5 | More Details |
| CVE-2020-16162 | An issue was discovered in RIPE NCC RPKI Validator 3.x through 3.1-2020.07.06.14.28. Missing validation checks on CRL presence or CRL staleness in the X509-based RPKI certificate-tree validation procedure allow remote attackers to bypass intended access restrictions by using revoked certificates. NOTE: there may be counterarguments related to backwards compatibility | 7.5 | More Details |
| CVE-2017-18923 | beroNet VoIP Gateways before 3.0.16 have a PHP script that allows downloading arbitrary files, including ones with credentials. | 7.5 | More Details |
| CVE-2020-7699 | This affects the package express-fileupload before 1.1.8. If the parseNested option is enabled, sending a corrupt HTTP request can lead to denial of service or arbitrary code execution. | 7.5 | More Details |
| CVE-2020-3700 | Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 | 7.5 | More Details |
| CVE-2020-6012 | ZoneAlarm Anti-Ransomware before version 1.0.713 copies files for the report from a directory with low privileges. A sophisticated timed attacker can replace those files with malicious or linked content, such as exploiting CVE-2020-0896 on unpatched systems or using symbolic links. This allows an unprivileged user to enable escalation of privilege via local access. | 7.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-16164 | An issue was discovered in RIPE NCC RPKI Validator 3.x through 3.1-2020.07.06.14.28. 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. NOTE: some third parties may regard this as a preferred behavior, not a vulnerability | 7.4 | More Details |
| CVE-2020-3376 | A vulnerability in the Device Manager application of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions on an affected device. The vulnerability is due to a failure in the software to perform proper authentication. An attacker could exploit this vulnerability by browsing to one of the hosted URLs in Cisco DCNM. A successful exploit could allow the attacker to interact with and use certain functions within the Cisco DCNM. | 7.3 | More Details |
| CVE-2020-11933 | cloud-init as managed by snapd on Ubuntu Core 16 and Ubuntu Core 18 devices was run without restrictions on every boot, which a physical attacker could exploit by crafting cloud-init user-data/meta-data via external media to perform arbitrary changes on the device to bypass intended security mechanisms such as full disk encryption. This issue did not affect traditional Ubuntu systems. Fixed in snapd version 2.45.2, revision 8539 and core version 2.45.2, revision 9659. | 7.3 | More Details |
| CVE-2020-8218 | A code injection vulnerability exists in Pulse Connect Secure <9.1R8 that allows an attacker to crafted a URI to perform an arbitrary code execution via the admin web interface. | 7.2 | More Details |
| CVE-2020-8219 | An insufficient permission check vulnerability exists in Pulse Connect Secure <9.1R8 that allows an attacker to change the password of a full administrator. | 7.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2019-14101 | Out of bounds read can happen in diag event set mask command handler when user provided length in the command request is less than expected length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS404, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 | 7.1 | More Details |
| CVE-2020-13522 | An exploitable arbitrary file delete vulnerability exists in SoftPerfect RAM Disk 4.1 spvve.sys driver. A specially crafted I/O request packet (IRP) can allow an unprivileged user to delete any file on the filesystem. An attacker can send a malicious IRP to trigger this vulnerability. | 7.1 | More Details |
| CVE-2020-8222 | A path traversal vulnerability exists in Pulse Connect Secure <9.1R8 that allowed an authenticated attacker via the administrator web interface to perform an arbitrary file reading vulnerability through Meeting. | 6.8 | More Details |
| CVE-2020-15135 | save-server (npm package) before version 1.05 is affected by a CSRF vulnerability, as there is no CSRF mitigation (Tokens etc.). The fix introduced in version version 1.05 unintentionally breaks uploading so version v1.0.7 is the fixed version. This is patched by implementing Double submit. The CSRF attack would require you to navigate to a malicious site while you have an active session with Save-Server (Session key stored in cookies). The malicious user would then be able to perform some actions, including uploading/deleting files and adding redirects. If you are logged in as root, this attack is significantly more severe. They can in addition create, delete and update users. If they updated the password of a user, that user's files would then be available. If the root password is updated, all files would be visible if they logged in with the new password. Note that due to the same origin policy malicious actors cannot view the gallery or the response of any of the methods, nor be sure they succeeded. This issue has been patched in version 1.0.7. | 6.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-7205 | A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. | 6.7 | More Details |
| CVE-2020-14309 | There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with name length of UINT32 bytes in size. The name size leads to an arithmetic overflow leading to a zero-size allocation further causing a heap-based buffer overflow with attacker controlled data. | 6.7 | More Details |
| CVE-2020-9248 | Huawei FusionComput 8.0.0 have an improper authorization vulnerability. A module does not verify some input correctly and authorizes files with incorrect access. Attackers can exploit this vulnerability to launch privilege escalation attack. This can compromise normal service. | 6.7 | More Details |
| CVE-2020-4569 | IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 uses a protection mechanism that relies on the existence or values of an input, but the input can be modified by an untrusted actor in a way that bypasses the protection mechanism. IBM X-Force ID: 184158. | 6.5 | More Details |
| CVE-2020-9689 | Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have a path traversal vulnerability. Successful exploitation could lead to arbitrary code execution. | 6.5 | More Details |
| CVE-2020-8192 | A denial of service vulnerability exists in Fastify v2.14.1 and v3.0.0-rc.4 that allows a malicious user to trigger resource exhaustion (when the allErrors option is used) with specially crafted schemas. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-2078 | Passwords are stored in plain text within the configuration of SICK Package Analytics software up to and including V04.1.1. An authorized attacker could access these stored plaintext credentials and gain access to the ftp service. Storing a password in plaintext allows attackers to easily gain access to systems, potentially compromising personal information or other sensitive information. | 6.5 | More Details |
| CVE-2020-9249 | HUAWEI P30 smartphones with versions earlier than 10.1.0.160(C00E160R2P11) have a denial of service vulnerability. A module does not deal with mal-crafted messages and it leads to memory leak. Attackers can exploit this vulnerability to make the device denial of service.Affected product versions include: HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11). | 6.5 | More Details |
| CVE-2020-8220 | A denial of service vulnerability exists in Pulse Connect Secure <9.1R8 that allows an authenticated attacker to perform command injection via the administrator web which can cause DOS. | 6.5 | More Details |
| CVE-2019-20032 | An attacker with access to an InMail voicemail box equipped with the find me/follow me feature on Aspire-derived NEC PBXes, including all versions of SV8100, SV9100, SL1100 and SL2100 devices, may access the system's administration modem. | 6.5 | More Details |
| CVE-2020-9692 | Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution. | 6.5 | More Details |
| CVE-2020-15705 | GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. | 6.4 | More Details |
| CVE-2020-15706 | GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. | 6.4 | More Details |
| CVE-2020-14308 | In grub2 versions before 2.06 the grub memory allocator doesn't check for possible arithmetic overflows on the requested allocation size. This leads the function to return invalid memory allocations which can be further used to cause possible integrity, confidentiality and availability impacts during the boot process. | 6.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-14486 | An attacker may bypass permission/authorization checks in OpenClinic GA 5.09.02 and 5.89.05b by ignoring the redirect of a permission failure, which may allow unauthorized execution of commands. | 6.3 | More Details |
| CVE-2020-3462 | A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database. | 6.3 | More Details |
| CVE-2020-4328 | IBM Financial Transaction Manager 3.2.4 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 177839. | 6.3 | More Details |
| CVE-2020-3377 | A vulnerability in the Device Manager application of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to inject arbitrary commands on the affected device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted arguments to a specific field within the application. A successful exploit could allow the attacker to run commands as the administrator on the DCNM. | 6.3 | More Details |
| CVE-2020-14489 | OpenClinic GA 5.09.02 and 5.89.05b stores passwords using inadequate hashing complexity, which may allow an attacker to recover passwords using known password cracking techniques. | 6.2 | More Details |
| CVE-2020-15129 | In Traefik before versions 1.7.26, 2.2.8, and 2.3.0-rc3, there exists a potential open redirect vulnerability in Traefik's handling of the "X-Forwarded-Prefix" header. The Traefik API dashboard component doesn't validate that the value of the header "X-Forwarded-Prefix" is a site relative path and will redirect to any header provided URI. Successful exploitation of an open redirect can be used to entice victims to disclose sensitive information. Active Exploitation of this issue is unlikely as it would require active header injection, however the Traefik team addressed this issue nonetheless to prevent abuse in e.g. cache poisoning scenarios. | 6.1 | More Details |
| CVE-2020-4560 | IBM Financial Transaction Manager 3.2.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2015-9549 | A reflected Cross-site Scripting (XSS) vulnerability exists in OcPortal 9.0.20 via the OCF_EMOTICON_CELL.tpl FIELD_NAME field to data/emoticons.php. | 6.1 | More Details |
| CVE-2020-13820 | Extreme Management Center 8.4.1.24 allows unauthenticated reflected XSS via a parameter in a GET request. | 6.1 | More Details |
| CVE-2020-16131 | Tiki before 21.2 allows XSS because [\s\/"\'] is not properly considered in lib/core/TikiFilter/PreventXss.php. | 6.1 | More Details |
| CVE-2020-11584 | A GET-based XSS reflected vulnerability in Plesk Onyx 17.8.11 allows remote unauthenticated users to inject arbitrary JavaScript, HTML, or CSS via a GET parameter. | 6.1 | More Details |
| CVE-2020-11583 | A GET-based XSS reflected vulnerability in Plesk Obsidian 18.0.17 allows remote unauthenticated users to inject arbitrary JavaScript, HTML, or CSS via a GET parameter. | 6.1 | More Details |
| CVE-2020-16847 | Extreme Analytics in Extreme Management Center before 8.5.0.169 allows unauthenticated reflected XSS via a parameter in a GET request, aka CFD-4887. | 6.1 | More Details |
| CVE-2020-16095 | The dlf (aka Kitodo.Presentation) extension before 3.1.2 for TYPO3 allows XSS. | 6.1 | More Details |
| CVE-2020-5612 | Cross-site scripting vulnerability in KonaWiki 2.2.0 and earlier allows remote attackers to execute an arbitrary script via a specially crafted URL. | 6.1 | More Details |
| CVE-2020-15128 | In OctoberCMS before version 1.0.468, encrypted cookie values were not tied to the name of the cookie the value belonged to. This meant that certain classes of attacks that took advantage of other theoretical vulnerabilities in user facing code (nothing exploitable in the core project itself) had a higher chance of succeeding. Specifically, if your usage exposed a way for users to provide unfiltered user input and have it returned to them as an encrypted cookie (ex. storing a user provided search query in a cookie) they could then use the generated cookie in place of other more tightly controlled cookies; or if your usage exposed the plaintext version of an encrypted cookie at any point to the user they could theoretically provide encrypted content from your application back to it as an encrypted cookie and force the framework to decrypt it for them. Issue has been fixed in build 468 (v1.0.468). | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-3460 | A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by intercepting a request from a user and injecting malicious data into an HTTP header. 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-2020-5613 | Cross-site scripting vulnerability in KonaWiki 3.1.0 and earlier allows remote attackers to execute an arbitrary script via a specially crafted URL. | 6.1 | More Details |
| CVE-2020-8204 | A cross site scripting (XSS) vulnerability exists in Pulse Connect Secure <9.1R5 on the PSAL Page. | 6.1 | More Details |
| CVE-2020-15870 | Sonatype Nexus Repository Manager OSS/Pro versions before 3.25.1 allow XSS (Issue 2 of 2). | 6.1 | More Details |
| CVE-2020-8553 | The Kubernetes ingress-nginx component prior to version 0.28.0 allows a user with the ability to create namespaces and to read and create ingress objects to overwrite the password file of another ingress which uses nginx.ingress.kubernetes.io/auth-type: basic and which has a hyphenated namespace or secret name. | 5.9 | More Details |
| CVE-2020-14319 | It was found that the AMQ Online console is vulnerable to a Cross-Site Request Forgery (CSRF) which is exploitable in cases where preflight checks are not instigated or bypassed. For example authorised users using an older browser with Adobe Flash are vulnerable when targeted by an attacker. This flaw affects all versions of AMQ-Online prior to 1.5.2 and Enmasse versions 0.31.0-rc1 up until but not including 0.32.2. | 5.9 | More Details |
| CVE-2020-16117 | In GNOME evolution-data-server before 3.35.91, a malicious server can crash the mail client with a NULL pointer dereference by sending an invalid (e.g., minimal) CAPABILITY line on a connection attempt. This is related to imapx_free_capability and imapx_connect_to_server. | 5.9 | More Details |
| CVE-2020-16843 | In Firecracker 0.20.x before 0.20.1 and 0.21.x before 0.21.2, the network stack can freeze under heavy ingress traffic. This can result in a denial of service on the microVM when it is configured with a single network interface, and an availability problem for the microVM network interface on which the issue is triggered. | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-16135 | libssh 0.9.4 has a NULL pointer dereference in tftpserver.c if ssh_buffer_new returns NULL. | 5.9 | More Details |
| CVE-2020-11934 | It was discovered that snapctl user-open allowed altering the $XDG_DATA_DIRS environment variable when calling the system xdg-open. OpenURL() in usersession/userd/launcher.go would alter $XDG_DATA_DIRS to append a path to a directory controlled by the calling snap. A malicious snap could exploit this to bypass intended access restrictions to control how the host system xdg-open script opens the URL and, for example, execute a script shipped with the snap without confinement. This issue did not affect Ubuntu Core systems. Fixed in snapd versions 2.45.1ubuntu0.2, 2.45.1+18.04.2 and 2.45.1+20.04.2. | 5.9 | More Details |
| CVE-2020-14337 | A data exposure flaw was found in Tower, where sensitive data was revealed from the HTTP return error codes. This flaw allows an unauthenticated, remote attacker to retrieve pages from the default organization and verify existing usernames. The highest threat from this vulnerability is to data confidentiality. | 5.8 | More Details |
| CVE-2020-14310 | There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow. | 5.7 | More Details |
| CVE-2020-15707 | Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. | 5.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-5414 | VMware Tanzu Application Service for VMs (2.7.x versions prior to 2.7.19, 2.8.x versions prior to 2.8.13, and 2.9.x versions prior to 2.9.7) contains an App Autoscaler that logs the UAA admin password. This credential is redacted on VMware Tanzu Operations Manager; however, the unredacted logs are available to authenticated users of the BOSH Director. This credential would grant administrative privileges to a malicious user. The same versions of App Autoscaler also log the App Autoscaler Broker password. Prior to newer versions of Operations Manager, this credential was not redacted from logs. This credential allows a malicious user to create, delete, and modify App Autoscaler services instances. Operations Manager started redacting this credential from logs as of its versions 2.7.15, 2.8.6, and 2.9.1. Note that these logs are typically only visible to foundation administrators and operators. | 5.7 | More Details |
| CVE-2020-14311 | There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow. | 5.7 | More Details |
| CVE-2020-4631 | IBM Spectrum Protect Plus 10.1.0 through 10.1.6 agent files, in non-default configurations, on Windows are assigned access to everyone with full control permissions, which could allow a local user to cause interruption of the service operations. IBM X-Force ID: 185372. | 5.5 | More Details |
| CVE-2020-16269 | radare2 4.5.0 misparses DWARF information in executable files, causing a segmentation fault in parse_typedef in type_dwarf.c via a malformed DW_AT_name in the .debug_info section. | 5.5 | More Details |
| CVE-2020-15944 | An issue was discovered in the Gantt-Chart module before 5.5.5 for Jira. Due to missing validation of user input, it is vulnerable to a persistent XSS attack. An attacker can embed the attack vectors in the dashboard of other users. To exploit this vulnerability, an attacker has to be authenticated. | 5.4 | More Details |
| CVE-2020-4542 | IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-force ID: 183046. | 5.4 | More Details |
| CVE-2020-4525 | IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 182435. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-4396 | IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 179359. | 5.4 | More Details |
| CVE-2020-16157 | A Stored XSS vulnerability exists in Nagios Log Server before 2.1.7 via the Notification Methods -> Email Users menu. | 5.4 | More Details |
| CVE-2020-8217 | A cross site scripting (XSS) vulnerability in Pulse Connect Secure <9.1R8 allowed attackers to exploit in the URL used for Citrix ICA. | 5.4 | More Details |
| CVE-2020-4644 | IBM Planning Analytics Local 2.0.0 through 2.0.9.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 185716. | 5.4 | More Details |
| CVE-2019-19453 | Wowza Streaming Engine before 4.8.5 allows XSS (issue 1 of 2). An authenticated user, with access to the proxy license editing is able to insert a malicious payload that will be triggered in the main page of server settings. This issue was resolved in Wowza Streaming Engine 4.8.5. | 5.4 | More Details |
| CVE-2020-15869 | Sonatype Nexus Repository Manager OSS/Pro versions before 3.25.1 allow XSS (issue 1 of 2). | 5.4 | More Details |
| CVE-2020-14492 | OpenClinic GA 5.09.02 and 5.89.05b does not properly neutralize user-controllable input, which may allow the execution of malicious code within the user’s browser. | 5.4 | More Details |
| CVE-2020-4645 | IBM Planning Analytics Local 2.0.0 through 2.0.9.1 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: 185717. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-15109 | In solidus before versions 2.8.6, 2.9.6, and 2.10.2, there is an bility to change order address without triggering address validations. This vulnerability allows a malicious customer to craft request data with parameters that allow changing the address of the current order without changing the shipment costs associated with the new shipment. All stores with at least two shipping zones and different costs of shipment per zone are impacted. This problem comes from how checkout permitted attributes are structured. We have a single list of attributes that are permitted across the whole checkout, no matter the step that is being submitted. See the linked reference for more information. As a workaround, if it is not possible to upgrade to a supported patched version, please use this gist in the references section. | 5.3 | More Details |
| CVE-2020-8202 | Improper check of inputs in Nextcloud Preferred Providers app v1.6.0 allowed to perform a denial of service attack when using a very long password. | 5.3 | More Details |
| CVE-2020-8213 | An information exposure vulnerability exists in UniFi Protect before v1.13.4-beta.5 that allowed unauthenticated attackers access to valid usernames for the UniFi Protect web application via HTTP response code and response timing. | 5.3 | More Details |
| CVE-2020-4573 | IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 could disclose sensitive information due to responding to unauthenticated HTTP requests. IBM X-Force ID: 184180. | 5.3 | More Details |
| CVE-2020-15511 | HashiCorp Terraform Enterprise up to v202006-1 contained a default signup page that allowed user registration even when disabled, bypassing SAML enforcement. Fixed in v202007-1. | 5.3 | More Details |
| CVE-2020-4572 | IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 184179. | 5.3 | More Details |
| CVE-2020-3461 | A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to obtain confidential information from an affected device. The vulnerability is due to missing authentication on a specific part of the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the interface. A successful exploit could allow the attacker to read confidential information from an affected device. | 5.3 | More Details |
| CVE-2019-4366 | IBM Cognos Analytics 11.0 and 11.1 is susceptible to an information disclosure vulnerability where an attacker could gain access to cached browser data. IBM X-Force ID: 161748. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-5614 | Directory traversal vulnerability in KonaWiki 3.1.0 and earlier allows remote attackers to read arbitrary files via unspecified vectors. | 5.3 | More Details |
| CVE-2020-12739 | A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. | 5.3 | More Details |
| CVE-2020-4186 | IBM Security Guardium 10.5, 10.6, and 11.1 could disclose sensitive information on the login page that could aid in further attacks against the system. IBM X-Force ID: 174804. | 5.3 | More Details |
| CVE-2020-8221 | A path traversal vulnerability exists in Pulse Connect Secure <9.1R8 which allows an authenticated attacker to read arbitrary files via the administrator web interface. | 4.9 | More Details |
| CVE-2020-8575 | Active IQ Unified Manager for VMware vSphere and Windows versions prior to 9.5 are susceptible to a vulnerability which allows administrative users to cause Denial of Service (DoS). | 4.4 | More Details |
| CVE-2020-8216 | An information disclosure vulnerability in meeting of Pulse Connect Secure <9.1R8 allowed an authenticated end-users to find meeting details, if they know the Meeting ID. | 4.3 | More Details |
| CVE-2020-4410 | IBM Jazz Foundation and IBM Engineering products could allow an authenticated user to send a specially crafted HTTP GET request to read attachments on the server that they should not have access to. IBM X-Force ID: 179539. | 4.3 | More Details |
| CVE-2019-4589 | IBM Cognos Analytics 11.0 and 11.1 is vulnerable to privlege escalation where the "My schedules and subscriptions" page is visible and accessible to a less privileged user. IBM X-Force ID: 167449. | 4.3 | More Details |
| CVE-2020-9690 | Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have an observable timing discrepancy vulnerability. Successful exploitation could lead to signature verification bypass. | 4.2 | More Details |
| CVE-2020-16166 | The Linux kernel through 5.7.11 allows remote attackers to make observations that help to obtain sensitive information about the internal state of the network RNG, aka CID-f227e3ec3b5c. This is related to drivers/char/random.c and kernel/time/timer.c. | 3.7 | More Details |
| CVE-2020-16201 | Delta Industrial Automation CNCSoft ScreenEditor, Versions 1.01.23 and prior. Multiple out-of-bounds read vulnerabilities may be exploited by processing specially crafted project files, which may allow an attacker to read information. | 3.3 | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2020-13523 | An exploitable information disclosure vulnerability exists in SoftPerfect's RAM Disk 4.1 spvve.sys driver. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability. | 3.3 | More Details |
| CVE-2020-16116 | In kerfuffle/jobs.cpp in KDE Ark before 20.08.0, a crafted archive can install files outside the extraction directory via ../ directory traversal. | 3.3 | More Details |