SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 02 September 2020

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-15164	in Scratch Login (MediaWiki extension) before version 1.1, any account can be logged into by using the same username with leading, trailing, or repeated underscore(s), since those are treated as whitespace and trimmed by MediaWiki. This affects all users on any wiki using this extension. Since version 1.1, comments by users whose usernames would be trimmed on MediaWiki are ignored when searching for the verification code.	10.0	More Details
CVE-2020-24653	secure-store in Expo through 2.16.1 on iOS provides the insecure kSecAttrAccessibleAlwaysThisDeviceOnly policy when WHEN_UNLOCKED_THIS_DEVICE_ONLY is used.	9.8	More Details
CVE-2020-7713	All versions of package arr-flatten-unflatten are vulnerable to Prototype Pollution via the constructor.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7714	All versions of package confucious are vulnerable to Prototype Pollution via the set function.	9.8	More Details
CVE-2020-7715	All versions of package deep-get-set are vulnerable to Prototype Pollution via the main function.	9.8	More Details
CVE-2020-7716	All versions of package deeps are vulnerable to Prototype Pollution via the set function.	9.8	More Details
CVE-2020-7717	All versions of package dot-notes are vulnerable to Prototype Pollution via the create function.	9.8	More Details
CVE-2020-7718	All versions of package gammautils are vulnerable to Prototype Pollution via the deepSet and deepMerge functions.	9.8	More Details
CVE-2020-7719	Versions of package locutus before 2.0.12 are vulnerable to prototype Pollution via the php.strings.parse_str function.	9.8	More Details
CVE-2020-7720	The package node-forge before 0.10.0 is vulnerable to Prototype Pollution via the util.setPath function. Note: Version 0.10.0 is a breaking change removing the vulnerable functions.	9.8	More Details
CVE-2020-7721	All versions of package node-oojs are vulnerable to Prototype Pollution via the setPath function.	9.8	More Details
CVE-2020-7722	All versions of package nodee-utils are vulnerable to Prototype Pollution via the deepSet function.	9.8	More Details
CVE-2020-7723	All versions of package promisehelpers are vulnerable to Prototype Pollution via the insert function.	9.8	More Details
CVE-2020-7724	All versions of package tiny-conf are vulnerable to Prototype Pollution via the set function.	9.8	More Details
CVE-2020-7725	All versions of package worksmith are vulnerable to Prototype Pollution via the setValue function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7726	All versions of package safe-object2 are vulnerable to Prototype Pollution via the setter function.	9.8	More Details
CVE-2020-25061	An issue was discovered on LG mobile devices with Android OS 9 and 10 software on the VZW network. lge_property allows property overwrites. The LG ID is LVE-SMP-200016 (July 2020).	9.8	More Details
CVE-2020-7727	All versions of package gedi are vulnerable to Prototype Pollution via the set function.	9.8	More Details
CVE-2020-6141	An exploitable SQL injection vulnerability exists in the login functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-16204	The affected product is vulnerable due to an undocumented interface found on the device, which may allow an attacker to execute commands as root on the device on the N-Tron 702-W / 702M12-W (all versions).	9.8	More Details
CVE-2020-25069	USVN (aka User-friendly SVN) before 1.0.10 allows attackers to execute arbitrary code in the commit view.	9.8	More Details
CVE-2020-5777	MAGMI versions prior to 0.7.24 are vulnerable to a remote authentication bypass due to allowing default credentials in the event there is a database connection failure. A remote attacker can trigger this connection failure if the Mysql setting max_connections (default 151) is lower than Apache (or another web server) setting MaxRequestWorkers (formerly MaxClients) (default 256). This can be done by sending at least 151 simultaneous requests to the Magento website to trigger a "Too many connections" error, then use default magmi:magmi basic authentication to remotely bypass authentication.	9.8	More Details
CVE-2020-6137	SQL injection vulnerability exists in the password reset functionality of OS4Ed openSIS 7.3. The password_stf_email parameter in the password reset page /opensis/ResetUserInfo.php is vulnerable to SQL injection. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-6138	SQL injection vulnerability exists in the password reset functionality of OS4Ed openSIS 7.3. The uname parameter in the password reset page /opensis/ResetUserInfo.php is vulnerable to SQL injection An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6139	SQL injection vulnerability exists in the password reset functionality of OS4Ed openSIS 7.3. The username_stf_email parameter in the password reset page /opensis/ResetUserInfo.php is vulnerable to SQL injection. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-6140	SQL injection vulnerability exists in the password reset functionality of OS4Ed openSIS 7.3. The password_stf_email parameter in the password reset page /opensis/ResetUserInfo.php is vulnerable to SQL injection. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-6142	A remote code execution vulnerability exists in the Modules.php functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can cause local file inclusion. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-6143	A remote code execution vulnerability exists in the install functionality of OS4Ed openSIS 7.4. The password variable which is set at line 122 in install/Step5.php allows for injection of PHP code into the Data.php file that it writes. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-6144	A remote code execution vulnerability exists in the install functionality of OS4Ed openSIS 7.4. The username variable which is set at line 121 in install/Step5.php allows for injection of PHP code into the Data.php file that it writes. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-6151	A memory corruption vulnerability exists in the TIFF handle_COMPRESSION_PACKBITS functionality of Accusoft ImageGear 19.7. A specially crafted malformed file can cause a memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2019-18847	Enterprise Access Client Auto-Updater allows for Remote Code Execution prior to version 2.0.1.	9.8	More Details
CVE-2020-25062	An issue was discovered on LG mobile devices with Android OS 9 and 10 software. LGTelephonyProvider allows a bypass of intended privilege restrictions. The LG ID is LVE-SMP-200017 (July 2020).	9.8	More Details
CVE-2020-25058	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9, and 10 software. The network_management service does not properly restrict configuration changes. The LG ID is LVE-SMP-200012 (July 2020).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5624	SQL injection vulnerability in the XooNIps 3.48 and earlier allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	9.8	More Details
CVE-2020-24007	Umanni RH 1.0 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-2020-3446	A vulnerability in Cisco Virtual Wide Area Application Services (vWAAS) with Cisco Enterprise NFV Infrastructure Software (NFVIS)-bundled images for Cisco ENCS 5400-W Series and CSP 5000-W Series appliances could allow an unauthenticated, remote attacker to log into the NFVIS CLI of an affected device by using accounts that have a default, static password. The vulnerability exists because the affected software has user accounts with default, static passwords. An attacker with access to the NFVIS CLI of an affected device could exploit this vulnerability by logging into the CLI. A successful exploit could allow the attacker to access the NFVIS CLI with administrator privileges.	9.8	More Details
CVE-2019-4694	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 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: 171832.	9.8	More Details
CVE-2020-23980	DesignMasterEvents Conference management 1.0.0 allows SQL Injection via the username field on the administrator login page.	9.8	More Details
CVE-2020-23973	KandNconcepts Club CMS 1.1 and 1.2 has SQL Injection via the 'team.php,player.php,club.php' id parameter.	9.8	More Details
CVE-2020-23976	Webexcels Ecommerce CMS 2.x, 2017, 2018, 2019, 2020 has SQL Injection via the 'content.php' id parameter.	9.8	More Details
CVE-2020-23978	SQL injection can occur in Soluzione Globale Ecommerce CMS v1 via the parameter " offerta.php"	9.8	More Details
CVE-2020-23979	13enforme CMS 1.0 has SQL Injection via the 'content.php' id parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24202	File Upload component in Projects World House Rental v1.0 suffers from an arbitrary file upload vulnerability with regular users, which allows remote attackers to conduct code execution.	9.8	More Details
CVE-2020-24203	Insecure File Permissions and Arbitrary File Upload in the upload pic function in updatesubcategory.php in Projects World Travel Management System v1.0 allows remote unauthenticated attackers to gain remote code execution.	9.8	More Details
CVE-2020-24714	The Scalyr Agent before 2.1.10 has Missing SSL Certificate Validation because, in some circumstances, the openssl binary is called without the -verify_hostname option.	9.8	More Details
CVE-2020-25057	An issue was discovered on LG mobile devices with Android OS 10 software. MDMService does not properly restrict APK installations. The LG ID is LVE-SMP-200011 (July 2020).	9.8	More Details
CVE-2020-24715	The Scalyr Agent before 2.1.10 has Missing SSL Certificate Validation because, in some circumstances, native Python code is used that lacks a comparison of the hostname to commonName and subjectAltName.	9.8	More Details
CVE-2020-7521	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in SFAPV9601 - APC Easy UPS On-Line Software (V2.0 and earlier) when accessing a vulnerable method of `FileUploadServlet` which may lead to uploading executable files to non-specified directories.	9.8	More Details
CVE-2020-25052	An issue was discovered on Samsung mobile devices with Q(10.0) (exynos9830 chipsets) software. H-Arx allows attackers to execute arbitrary code or cause a denial of service (memory corruption) because indexes are mishandled. The Samsung ID is SVE-2020-17426 (August 2020).	9.8	More Details
CVE-2020-25020	MPXJ through 8.1.3 allows XXE attacks. This affects the GanttProjectReader and PhoenixReader components.	9.8	More Details
CVE-2020-24115	In projectworlds Online Book Store 1.0 Use of Hard-coded Credentials in source code leads to admin panel access.	9.8	More Details
CVE-2020-12645	OX App Suite 7.10.1 to 7.10.3 has improper input validation for rate limits with a crafted User-Agent header, spoofed vacation notices, and /apps/load memory consumption.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25055	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The persona service allows attackers (who control an unprivileged SecureFolder process) to bypass admin restrictions in KnoxContainer. The Samsung ID is SVE-2020-18133 (August 2020).	9.8	More Details
CVE-2020-24786	An issue was discovered in Zoho ManageEngine Exchange Reporter Plus before build number 5510, AD360 before build number 4228, ADSelfService Plus before build number 5817, DataSecurity Plus before build number 6033, RecoverManager Plus before build number 6017, EventLog Analyzer before build number 12136, ADAudit Plus before build number 6052, O365 Manager Plus before build number 4334, Cloud Security Plus before build number 4110, ADManager Plus before build number 7055, and Log360 before build number 5166. The remotely accessible Java servlet com.manageengine.ads.fw.servlet.UpdateProductDetails is prone to an authentication bypass. System integration properties can be modified and lead to full ManageEngine suite compromise.	9.8	More Details
CVE-2020-25053	An issue was discovered on Samsung mobile devices with Q(10.0) (exynos9830 chipsets) software. RKP allows arbitrary code execution. The Samsung ID is SVE-2020-17435 (August 2020).	9.8	More Details
CVE-2020-7522	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in SFAPV9601 - APC Easy UPS On-Line Software (V2.0 and earlier) when accessing a vulnerable method of `SoundUploadServlet` which may lead to uploading executable files to non-specified directories.	9.8	More Details
CVE-2020-25049	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. StatusBarService has insufficient DEX access control. The Samsung ID is SVE-2020-17797 (August 2020).	9.8	More Details
CVE-2020-14498	HMS Industrial Networks AB eCatcher all versions prior to 6.5.5 is vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute arbitrary code.	9.6	More Details
CVE-2020-25067	NETGEAR R8300 devices before 1.0.2.134 are affected by command injection by an unauthenticated attacker.	9.6	More Details
CVE-2020-15165	Version 1.1.6-free of Chameleon Mini Live Debugger on Google Play Store may have had it's sources or permissions tampered by a malicious actor. The official maintainer of the package is recommending all users upgrade to v1.1.8 as soon as possible. For more information, review the referenced GitHub Security Advisory.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25016	A safety violation was discovered in the rgb crate before 0.8.20 for Rust, leading to (for example) dereferencing of arbitrary pointers or disclosure of uninitialized memory. This occurs because structs can be treated as bytes for read and write operations.	9.1	More Details
CVE-2020-25054	An issue was discovered on Samsung mobile devices with software through 2020-04-02 (Exynos modem chipsets). There is a heap-based buffer over-read in the Shannon baseband. The Samsung ID is SVE-2020-17239 (August 2020).	9.1	More Details
CVE-2020-6874	A ZTE product is impacted by the cryptographic issues vulnerability. The encryption algorithm is not properly used, so remote attackers could use this vulnerability for account credential enumeration attack or brute-force attack for password guessing. This affects: ZXIPTV, ZXIPTV-WEB-PV5.09.08.04.	9.1	More Details
CVE-2020-16210	The affected product is vulnerable to reflected cross-site scripting, which may allow an attacker to remotely execute arbitrary code and perform actions in the context of an attacked user on the N-Tron 702-W / 702M12-W (all versions).	9.0	More Details
CVE-2020-16206	The affected product is vulnerable to stored cross-site scripting, which may allow an attacker to remotely execute arbitrary code to gain access to sensitive data on the N-Tron 702-W / 702M12-W (all versions).	9.0	More Details
CVE-2020-15150	There is a vulnerability in Paginator (Elixir/Hex package) which makes it susceptible to Remote Code Execution (RCE) attacks via input parameters to the paginate() function. This will potentially affect all current users of Paginator prior to version 1.0.0. The vulnerability has been patched in version 1.0.0 and all users should upgrade to this version immediately. Note that this patched version uses a dependency that requires an Elixir version >=1.5.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-24897	The Table Filter and Charts for Confluence Server app before 5.3.25 (for Atlassian Confluence) allow remote attackers to inject arbitrary HTML or JavaScript via cross site scripting (XSS) through the provided Markdown markup to the "Table from CSV" macro.	8.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6131	SQL injection vulnerabilities exist in the course_period_id parameters used in OS4Ed openSIS 7.3 pages. The course_period_id parameter in the page MassScheduleSessionSet.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.	8.8	More Details
CVE-2020-6132	SQL injection vulnerability exists in the ID parameters of OS4Ed openSIS 7.3 pages. The id parameter in the page ChooseCP.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-10518	A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration of the underlying parsers used by GitHub Pages were not sufficiently restricted and made it possible to execute commands on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22 and was fixed in 2.21.6, 2.20.15, and 2.19.21. The underlying issues contributing to this vulnerability were identified both internally and through the GitHub Security Bug Bounty program.	8.8	More Details
CVE-2020-6127	SQL injection vulnerability exists in the CoursePeriodModal.php page of OS4Ed openSIS 7.3. The id parameter in the page CoursePeriodModal.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-6126	SQL injection vulnerability exists in the CoursePeriodModal.php page of OS4Ed openSIS 7.3. The course_period_id parameter in the page CoursePeriodModal.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.	8.8	More Details
CVE-2020-6125	An exploitable SQL injection vulnerability exists in the GetSchool.php functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-6124	An exploitable sql injection vulnerability exists in the email parameter functionality of OS4Ed openSIS 7.3. The email parameter in the page EmailCheckOthers.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6130	SQL injection vulnerabilities exist in the course_period_id parameters used in OS4Ed openSIS 7.3 pages. The course_period_id parameter in the page MassDropSessionSet.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.	8.8	More Details
CVE-2020-6129	SQL injection vulnerabilities exist in the course_period_id parameters used in OS4Ed openSIS 7.3 pages. The course_period_id parameter in the page CpSessionSet.php is vulnerable to SQL injection.An attacker can make an authenticated HTTP request to trigger these vulnerabilities.	8.8	More Details
CVE-2020-3443	A vulnerability in Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an authenticated, remote attacker to elevate privileges and execute commands with higher privileges. The vulnerability is due to insufficient authorization of the System Operator role capabilities. An attacker could exploit this vulnerability by logging in with the System Operator role, performing a series of actions, and then assuming a new higher privileged role. A successful exploit could allow the attacker to perform all actions associated with the privilege of the assumed role. If that role is an administrative role, the attacker would gain full access to the device.	8.8	More Details
CVE-2020-6123	An exploitable sql injection vulnerability exists in the email parameter functionality of OS4Ed openSIS 7.3. The email parameter in the page EmailCheck.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-6122	SQL injection vulnerability exists in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The mn parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-6121	SQL injection vulnerabilities exist in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The ln parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-6120	SQL injection vulnerability exists in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The fn parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-6119	SQL injection vulnerabilities exist in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The byear parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6118	SQL injection vulnerabilities exist in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The bmonth parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-6117	SQL injection vulnerabilities exist in the CheckDuplicateStudent.php page of OS4Ed openSIS 7.3. The bday parameter in the page CheckDuplicateStudent.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-3506	Multiple vulnerabilities in the Cisco Discovery Protocol implementation for Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP camera. These vulnerabilities are due to missing checks when the IP cameras process a Cisco Discovery Protocol packet. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to the targeted IP camera. A successful exploit could allow the attacker to execute code on the affected IP camera or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	8.8	More Details
CVE-2020-3507	Multiple vulnerabilities in the Cisco Discovery Protocol implementation for Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP camera. These vulnerabilities are due to missing checks when the IP cameras process a Cisco Discovery Protocol packet. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to the targeted IP camera. A successful exploit could allow the attacker to execute code on the affected IP camera or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	8.8	More Details
CVE-2020-2241	A cross-site request forgery (CSRF) vulnerability in Jenkins database Plugin 1.6 and earlier allows attackers to connect to an attacker-specified database server using attacker-specified credentials.	8.8	More Details
CVE-2020-2240	A cross-site request forgery (CSRF) vulnerability in Jenkins database Plugin 1.6 and earlier allows attackers to execute arbitrary SQL scripts.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3415	A vulnerability in the Data Management Engine (DME) of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code with administrative privileges or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to a Layer 2-adjacent affected device. A successful exploit could allow the attacker to execute arbitrary code with administrative privileges or cause the Cisco Discovery Protocol process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition. Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Exploitation of this vulnerability also requires jumbo frames to be enabled on the interface that receives the crafted Cisco Discovery Protocol packets on the affected device.	8.8	More Details
CVE-2020-24972	The Kleopatra component before 3.1.12 (and before 20.07.80) for GnuPG allows remote attackers to execute arbitrary code because openpgp4fpr: URLs are supported without safe handling of command-line options. The Qt platformpluginpath command-line option can be used to load an arbitrary DLL.	8.8	More Details
CVE-2020-13593	The Bluetooth Low Energy Secure Manager Protocol (SMP) implementation in Texas Instruments SimpleLink SIMPLELINK-CC2640R2-SDK through 2.2.3 allows the Diffie-Hellman check during the Secure Connection pairing to be skipped if the Link Layer encryption setup is performed earlier. An attacker in radio range can achieve arbitrary read/write access to protected GATT service data, cause a denial of service, or possibly control a device's function by establishing an encrypted session with an unauthenticated Long Term Key (LTK).	8.8	More Details
CVE-2019-5321	Aruba Intelligent Edge Switch Series 2540, 2530, 2930F, 2930M, 2920, 5400R, and 3810M with firmware 16.08.* before 16.08.0009, 16.09.* before 16.09.0007, 16.10.* before 16.10.0003 are vulnerable to Remote Unauthorized Access in the WebUI.	8.8	More Details
CVE-2020-24363	TP-Link TL-WA855RE V5 20200415-rel37464 devices allow an unauthenticated attacker (on the same network) to submit a TDDP_RESET POST request for a factory reset and reboot. The attacker can then obtain incorrect access control by setting a new administrative password.	8.8	More Details
CVE-2020-24354	Zyxel VMG5313-B30B router on firmware 5.13(ABCJ.6)b3_1127, and possibly older versions of firmware are affected by shell injection.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-4713	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 172084.	8.8	More Details
CVE-2020-12456	A remote code execution vulnerability in Mitel MiVoice Connect Client before 214.100.1223.0 could allow an attacker to execute arbitrary code in the chat notification window, due to improper rendering of chat messages. A successful exploit could allow an attacker to steal session cookies, perform directory traversal, and execute arbitrary scripts in the context of the Connect client.	8.8	More Details
CVE-2020-12855	A Host header injection vulnerability has been discovered in SecZetta NEProfile 3.3.11. Authenticated remote adversaries can poison this header resulting in an adversary controlling the execution flow for the 302 HTTP status.	8.8	More Details
CVE-2020-6128	SQL injection vulnerability exists in the CoursePeriodModal.php page of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. The meet_date parameter in the page CoursePeriodModal.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-7526	Improper Input Validation vulnerability exists in PowerChute Business Edition (software V9.0.x and earlier) which could cause remote code execution when a script is executed during a shutdown event.	8.8	More Details
CVE-2020-6133	SQL injection vulnerabilities exist in the ID parameters of OS4Ed openSIS 7.3 pages. The id parameter in the page CourseMoreInfo.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-17405	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Senstar Symphony 7.3.2.2. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SSOAuth process. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10980.	8.8	More Details
CVE-2020-23836	A Cross-Site Request Forgery (CSRF) vulnerability in edit_user.php in OSWAPP Warehouse Inventory System (aka OSWA-INV) through 2020-08-10 allows remote attackers to change the admin's password after an authenticated admin visits a third-party site.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24703	An issue was discovered in certain WSO2 products. A valid Carbon Management Console session cookie may be sent to an attacker-controlled server if the victim submits a crafted Try It request, aka Session Hijacking. This affects API Manager 2.2.0, API Manager Analytics 2.2.0, API Microgateway 2.2.0, Data Analytics Server 3.2.0, Enterprise Integrator through 6.6.0, IS as Key Manager 5.5.0, Identity Server 5.5.0 and 5.8.0, Identity Server Analytics 5.5.0, and IoT Server 3.3.0 and 3.3.1.	8.8	More Details
CVE-2020-24705	An issue was discovered in certain WSO2 products. A valid Carbon Management Console session cookie may be sent to an attacker-controlled server if the victim submits a crafted Try It request, aka Session Hijacking. This affects API Manager through 3.1.0, API Manager Analytics 2.5.0, IS as Key Manager through 5.10.0, Identity Server through 5.10.0, Identity Server Analytics through 5.6.0, and IoT Server 3.1.0.	8.8	More Details
CVE-2020-24034	Sagemcom F@ST 5280 routers using firmware version 1.150.61 have insecure deserialization that allows any authenticated user to perform a privilege escalation to any other user. By making a request with valid sess_id, nonce, and ha1 values inside of the serialized session cookie, an attacker may alter the user value inside of this cookie, and assume the role and permissions of the user specified. By assuming the role of the user internal, which is inaccessible to end users by default, the attacker gains the permissions of the internal account, which includes the ability to flash custom firmware to the router, allowing the attacker to achieve a complete compromise.	8.8	More Details
CVE-2020-23829	interface/new/new_comprehensive_save.php in LibreHealth EHR 2.0.0 suffers from an authenticated file upload vulnerability, allowing remote attackers to achieve remote code execution (RCE) on the hosting webserver by uploading a maliciously crafted image.	8.8	More Details
CVE-2020-6136	An exploitable SQL injection vulnerability exists in the DownloadWindow.php functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-16208	The affected product is vulnerable to cross-site request forgery, which may allow an attacker to modify different configurations of a device by luring an authenticated user to click on a crafted link on the N-Tron 702-W / 702M12-W (all versions).	8.8	More Details
CVE-2020-5922	In BIG-IP versions 15.0.0-15.1.0.4, 14.1.0-14.1.2.6, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.2, iControl REST does not implement Cross Site Request Forgery protections for users which make use of Basic Authentication in a web browser.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2012-3336	IBM InfoSphere Guardium 8.0, 8.01, and 8.2 is vulnerable to SQL injection. A remote authenticated attacker could send specially-crafted SQL statements to multiple scripts, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 78282.	8.8	More Details
CVE-2020-6134	SQL injection vulnerabilities exist in the ID parameters of OS4Ed openSIS 7.3 pages. The id parameter in the page MassDropModal.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-25070	USVN (aka User-friendly SVN) before 1.0.10 allows CSRF, related to the lack of the SameSite Strict feature.	8.8	More Details
CVE-2020-5776	Currently, all versions of MAGMI are vulnerable to CSRF due to the lack of CSRF tokens. RCE (via phpcli command) is possible in the event that a CSRF is leveraged against an existing admin session for MAGMI.	8.8	More Details
CVE-2020-6135	An exploitable SQL injection vulnerability exists in the Validator.php functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-3517	A vulnerability in the Cisco Fabric Services component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated attacker to cause process crashes, which could result in a denial of service (DoS) condition on an affected device. The attack vector is configuration dependent and could be remote or adjacent. For more information about the attack vector, see the Details section of this advisory. The vulnerability is due to insufficient error handling when the affected software parses Cisco Fabric Services messages. An attacker could exploit this vulnerability by sending malicious Cisco Fabric Services messages to an affected device. A successful exploit could allow the attacker to cause a reload of an affected device, which could result in a DoS condition.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3397	A vulnerability in the Border Gateway Protocol (BGP) Multicast VPN (MVPN) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an affected device to unexpectedly reload, resulting in a denial of service (DoS) condition. The vulnerability is due to incomplete input validation of a specific type of BGP MVPN update message. An attacker could exploit this vulnerability by sending this specific, valid BGP MVPN update message to a targeted device. A successful exploit could allow the attacker to cause one of the BGP-related routing applications to restart multiple times, leading to a system-level restart. Note: The Cisco implementation of BGP accepts incoming BGP traffic from only explicitly configured peers. To exploit this vulnerability, an attacker must send a specific BGP MVPN update message over an established TCP connection that appears to come from a trusted BGP peer. To do so, the attacker must obtain information about the BGP peers in the trusted network of the affected system.	8.6	More Details
CVE-2020-3398	A vulnerability in the Border Gateway Protocol (BGP) Multicast VPN (MVPN) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a BGP session to repeatedly reset, causing a partial denial of service (DoS) condition due to the BGP session being down. The vulnerability is due to incorrect parsing of a specific type of BGP MVPN update message. An attacker could exploit this vulnerability by sending this BGP MVPN update message to a targeted device. A successful exploit could allow the attacker to cause the BGP peer connections to reset, which could lead to BGP route instability and impact traffic. The incoming BGP MVPN update message is valid but is parsed incorrectly by the NX-OS device, which could send a corrupted BGP update to the configured BGP peer. Note: The Cisco implementation of BGP accepts incoming BGP traffic from only explicitly configured peers. To exploit this vulnerability, an attacker must send a specific BGP MVPN update message over an established TCP connection that appears to come from a trusted BGP peer. To do so, the attacker must obtain information about the BGP peers in the trusted network of the affected system.	8.6	More Details
CVE-2020-3566	A vulnerability in the Distance Vector Multicast Routing Protocol (DVMRP) feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to exhaust process memory of an affected device. The vulnerability is due to insufficient queue management for Internet Group Management Protocol (IGMP) packets. An attacker could exploit this vulnerability by sending crafted IGMP traffic to an affected device. A successful exploit could allow the attacker to cause memory exhaustion, resulting in instability of other processes. These processes may include, but are not limited to, interior and exterior routing protocols. Cisco will release software updates that address this vulnerability.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17376	An issue was discovered in Guest.migrate in virt/libvirt/guest.py in OpenStack Nova before 19.3.1, 20.x before 20.3.1, and 21.0.0. By performing a soft reboot of an instance that has previously undergone live migration, a user may gain access to destination host devices that share the same paths as host devices previously referenced by the virtual machine on the source host. This can include block devices that map to different Cinder volumes at the destination than at the source. Only deployments allowing host-based connections (for instance, root and ephemeral devices) are affected.	8.3	More Details
CVE-2020-16251	HashiCorp Vault and Vault Enterprise versions 0.8.3 and newer, when configured with the GCP GCE auth method, may be vulnerable to authentication bypass. Fixed in 1.2.5, 1.3.8, 1.4.4, and 1.5.1.	8.2	More Details
CVE-2020-16250	HashiCorp Vault and Vault Enterprise versions 0.7.1 and newer, when configured with the AWS IAM auth method, may be vulnerable to authentication bypass. Fixed in 1.2.5, 1.3.8, 1.4.4, and 1.5.1..	8.2	More Details
CVE-2020-8097	An improper authentication vulnerability in Bitdefender Endpoint Security Tools for Windows and Bitdefender Endpoint Security SDK allows an unprivileged local attacker to escalate privileges or tamper with the product's security settings. This issue affects: Bitdefender Endpoint Security Tools for Windows versions prior to 6.6.18.261. This issue affects: Bitdefender Endpoint Security Tools for Windows versions prior to 6.6.18.261. Bitdefender Endpoint Security SDK versions prior to 6.6.18.261.	8.1	More Details
CVE-2020-15601	If LDAP authentication is enabled, an LDAP authentication bypass vulnerability in Trend Micro Deep Security 10.x-12.x could allow an unauthenticated attacker with prior knowledge of the targeted organization to bypass manager authentication. Enabling multi-factor authentication prevents this attack. Installations using manager native authentication or SAML authentication are not impacted by this vulnerability.	8.1	More Details
CVE-2020-3519	A vulnerability in a specific REST API method of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct a path traversal attack on an affected device. 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 overwrite arbitrary files on the affected device.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13863	The SAS portal of Mitel MiCollab before 9.1.3 could allow an attacker to access user data by performing a header injection in HTTP responses, due to the improper handling of input parameters. A successful exploit could allow an attacker to access user information.	8.1	More Details
CVE-2020-15605	If LDAP authentication is enabled, an LDAP authentication bypass vulnerability in Trend Micro Vulnerability Protection 2.0 SP2 could allow an unauthenticated attacker with prior knowledge of the targeted organization to bypass manager authentication. Enabling multi-factor authentication prevents this attack. Installations using manager native authentication or SAML authentication are not impacted by this vulnerability.	8.1	More Details
CVE-2020-14352	A flaw was found in librepo in versions before 1.12.1. A directory traversal vulnerability was found where it failed to sanitize paths in remote repository metadata. An attacker controlling a remote repository may be able to copy files outside of the destination directory on the targeted system via path traversal. This flaw could potentially result in system compromise via the overwriting of critical system files. The highest threat from this flaw is to users that make use of untrusted third-party repositories.	8.0	More Details
CVE-2020-11618	THOMSON THT741FTA 2.2.1 and Philips DTR3502BFTA DVB-T2 2.2.1 set-top boxes have their TELNET service hardcoded to start on boot, which allows an attacker on the local network to achieve root access via the TELNET protocol.	7.8	More Details
CVE-2020-24559	A vulnerability in Trend Micro Apex One, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services on macOS may allow an attacker to manipulate a certain binary to load and run a script from a user-writable folder, which then would allow them to execute arbitrary code as root. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2020-6152	A code execution vulnerability exists in the DICOM parse_dicom_meta_info functionality of Accusoft ImageGear 19.7. A specially crafted malformed file can cause an out-of-bounds write. An attacker can trigger this vulnerability by providing a victim with a malicious DICOM file.	7.8	More Details
CVE-2020-15482	An issue was discovered on Nescomed Multipara Monitor M1000 devices. The device enables an unencrypted TELNET service by default, with a blank password for the admin account. This allows an attacker to gain root access to the device over the local network.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7523	Improper Privilege Management vulnerability exists in Schneider Electric Modbus Serial Driver (see security notification for versions) which could cause local privilege escalation when the Modbus Serial Driver service is invoked. The driver does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor.	7.8	More Details
CVE-2020-25031	checkinstall 1.6.2, when used to create a package that contains a symlink, may trigger the creation of a mode 0777 executable file.	7.8	More Details
CVE-2020-24955	SUPERAntiSyware Professional X Trial 10.0.1206 is vulnerable to local privilege escalation because it allows unprivileged users to restore a malicious DLL from quarantine into the system32 folder via an NTFS directory junction, as demonstrated by a crafted ualapi.dll file that is detected as malware.	7.8	More Details
CVE-2020-7527	Incorrect Default Permission vulnerability exists in SoMove (V2.8.1) and prior which could cause elevation of privilege and provide full access control to local system users to SoMove component and services when a SoMove installer script is launched.	7.8	More Details
CVE-2020-25060	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. Local users can gain privileges because of LAF and SBL1 flaws. The LG ID is LVE-SMP-200015 (July 2020).	7.8	More Details
CVE-2020-24716	OpenZFS before 2.0.0-rc1, when used on FreeBSD, allows execute permissions for all directories.	7.8	More Details
CVE-2020-24717	OpenZFS before 2.0.0-rc1, when used on FreeBSD, misinterprets group permissions as user permissions, as demonstrated by mode 0770 being equivalent to mode 0777.	7.8	More Details
CVE-2020-24556	A vulnerability in Trend Micro Apex One, OfficeScan XG SP1, Worry-Free Business Security 10 SP1 and Worry-Free Business Security Services on Microsoft Windows may allow an attacker to create a hard link to any file on the system, which then could be manipulated to gain a privilege escalation and code execution. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3394	A vulnerability in the Enable Secret feature of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an authenticated, local attacker to issue the enable command and get full administrative privileges. To exploit this vulnerability, the attacker would need to have valid credentials for the affected device. The vulnerability is due to a logic error in the implementation of the enable command. An attacker could exploit this vulnerability by logging in to the device and issuing the enable command. A successful exploit could allow the attacker to gain full administrative privileges without using the enable password. Note: The Enable Secret feature is disabled by default.	7.8	More Details
CVE-2020-24557	A vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 on Microsoft Windows may allow an attacker to manipulate a particular product folder to disable the security temporarily, abuse a specific Windows function and attain privilege escalation. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected.	7.8	More Details
CVE-2020-15158	In libIEC61850 before version 1.4.3, when a message with COTP message length field with value < 4 is received an integer underflow will happen leading to heap buffer overflow. This can cause an application crash or on some platforms even the execution of remote code. If your application is used in open networks or there are untrusted nodes in the network it is highly recommend to apply the patch. This was patched with commit 033ab5b. Users of version 1.4.x should upgrade to version 1.4.3 when available. As a workaround changes of commit 033ab5b can be applied to older versions.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8023	A acceptance of Extraneous Untrusted Data With Trusted Data vulnerability in the start script of openldap2 of SUSE Enterprise Storage 5, SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SECURITY, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to escalate privileges from user ldap to root. This issue affects: SUSE Enterprise Storage 5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Debuginfo 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Debuginfo 11-SP4 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Point of Sale 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 11-SECURITY openldap2-client-openssl1 versions prior to 2.4.26-0.74.13.1. SUSE Linux Enterprise Server 11-SP4-LTSS openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 12-SP2-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP2-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP4 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP5 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.31.1. SUSE Linux Enterprise Server for SAP 12-SP2 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 12-SP3 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.31.1. SUSE OpenStack Cloud 7 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud 8 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud Crowbar 8 openldap2 versions prior to 2.4.41-18.71.2. openSUSE Leap 15.1 openldap2 versions prior to 2.4.46-lp151.10.12.1. openSUSE Leap 15.2 openldap2 versions prior to 2.4.46-lp152.14.3.1.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15159	baserCMS 4.3.6 and earlier is affected by Cross Site Scripting (XSS) and Remote Code Execution (RCE). This may be executed by logging in as a system administrator and uploading an executable script file such as a PHP file.The affected components are ThemeFilesController.php and UploaderFilesController.php. This is fixed in version 4.3.7.	7.6	More Details
CVE-2020-24898	The Table Filter and Charts for Confluence Server app before 5.3.26 (for Atlassian Confluence) allows SSRF via the "Table from CSV" macro (URL parameter).	7.6	More Details
CVE-2020-15687	Missing access control restrictions in the Hypervisor component of the ACRN Project (v2.0 and v1.6.1) allow a malicious entity, with root access in the Service VM userspace, to abuse the PCIe assign/de-assign Hypercalls via crafted ioctls and payloads. This attack results in a corrupt state and Denial of Service (DoS) for previously assigned PCIe devices to the Service VM at runtime.	7.5	More Details
CVE-2020-20625	Sliced Invoices plugin for WordPress 3.8.2 and earlier allows unauthenticated information disclosure and authenticated SQL injection via core/class-sliced.php.	7.5	More Details
CVE-2020-4169	IBM Security Guardium Insights 2.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174405.	7.5	More Details
CVE-2020-9298	The Spinnaker template resolution functionality is vulnerable to Server-Side Request Forgery (SSRF), which allows an attacker to send requests on behalf of Spinnaker potentially leading to sensitive data disclosure.	7.5	More Details
CVE-2020-25032	An issue was discovered in Flask-CORS (aka CORS Middleware for Flask) before 3.0.9. It allows ../ directory traversal to access private resources because resource matching does not ensure that pathnames are in a canonical format.	7.5	More Details
CVE-2020-7524	Out-of-bounds Write vulnerability exists in Modicon M218 Logic Controller (V5.0.0.7 and prior) which could cause Denial of Service when sending specific crafted IPV4 packet to the controller: Sending a specific IPv4 protocol package to Schneider Electric Modicon M218 Logic Controller can cause IPv4 devices to go down. The device does not work properly and must be powered back on to return to normal.	7.5	More Details
CVE-2020-4174	IBM Security Guardium Insights 2.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174683.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3338	A vulnerability in the Protocol Independent Multicast (PIM) feature for IPv6 networks (PIM6) of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper error handling when processing inbound PIM6 packets. An attacker could exploit this vulnerability by sending multiple crafted PIM6 packets to an affected device. A successful exploit could allow the attacker to cause the PIM6 application to leak system memory. Over time, this memory leak could cause the PIM6 application to stop processing legitimate PIM6 traffic, leading to a DoS condition on the affected device.	7.5	More Details
CVE-2020-25019	jitsi-meet-electron (aka Jitsi Meet Electron) before 2.3.0 calls the Electron shell.openExternal function without verifying that the URL is for an http or https resource, in some circumstances.	7.5	More Details
CVE-2020-7525	Improper Restriction of Excessive Authentication Attempts vulnerability exists in all hardware versions of spaceLYnk and Wiser for KNX (formerly homeLYnk) which could allow an attacker to guess a password when brute force is used.	7.5	More Details
CVE-2020-23972	In Joomla Component GMapFP Version J3.5 and J3.5free, an attacker can access the upload function without authenticating to the application and can also upload files which due to issues of unrestricted file uploads which can be bypassed by changing the content-type and name file too double extensions.	7.5	More Details
CVE-2020-4559	IBM Spectrum Protect 7.1 and 8.1 could allow an attacker to cause a denial of service due ti improper validation of user-supplied input. IBM X-Force ID: 183613.	7.5	More Details
CVE-2020-11797	An Authentication Bypass vulnerability in the Published Area of the web conferencing component of Mitel MiCollab AWV before 8.1.2.4 and 9.x before 9.1.3 could allow an unauthenticated attacker to gain access to unauthorized information due to insufficient access validation. A successful exploit could allow an attacker to access sensitive shared files.	7.5	More Details
CVE-2020-7665	This affects all versions of package github.com/u-root/u-root/pkg/uzip. It is vulnerable to both leading and non-leading relative path traversal attacks in zip file extraction.	7.5	More Details
CVE-2020-24312	mndpsingh287 WP File Manager v6.4 and lower fails to restrict external access to the fm_backups directory with a .htaccess file. This results in the ability for unauthenticated users to browse and download any site backups, which sometimes include full database backups, that the plugin has taken.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24315	Vinoj Cardoza WordPress Poll Plugin v36 and lower executes SQL statement passed in via the pollid POST parameter due to a lack of user input escaping. This allows users who craft specific SQL statements to dump the entire targets database.	7.5	More Details
CVE-2020-13410	An issue was discovered in MoscaJS Aedes 0.42.0. lib/write.js does not properly consider exceptions during the writing of an invalid packet to a stream.	7.5	More Details
CVE-2020-15484	An issue was discovered on Nescomed Multipara Monitor M1000 devices. The internal storage of the underlying Linux system stores data in cleartext, without integrity protection against tampering.	7.5	More Details
CVE-2020-5914	In BIG-IP ASM versions 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, 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, undisclosed server cookie scenario may cause BD to restart under some circumstances.	7.5	More Details
CVE-2020-5918	In BIG-IP versions 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, 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, the Traffic Management Microkernel (TMM) may stop responding when processing Stream Control Transmission Protocol (SCTP) traffic when traffic volume is high. This vulnerability affects TMM by way of a virtual server configured with an SCTP profile.	7.5	More Details
CVE-2020-5919	In versions 15.1.0-15.1.0.4, rendering of certain session variables by BIG-IP APM UI-based agents in an access profile configured with Modern customization, may cause the Traffic Management Microkernel (TMM) to stop responding.	7.5	More Details
CVE-2020-23971	gmapfp.org Joomla Component GMapFP J3.30pro is affected by Insecure Permissions. An attacker can access the upload function without authenticating to the application and also can upload files due the issues of unrestricted file uploads which can be bypassed by changing the content-type and name file too double extensions.	7.5	More Details
CVE-2020-5921	in BIG-IP versions 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, 13.1.0-13.1.3.4, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.2, Syn flood causes large number of MCPD context messages destined to secondary blades consuming memory leading to MCPD failure. This issue affects only VIPRION hosts with two or more blades installed. Single-blade VIPRION hosts are not affected.	7.5	More Details
CVE-2020-5925	In BIG-IP versions 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, undisclosed internally generated UDP traffic may cause the Traffic Management Microkernel (TMM) to restart under some circumstances.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5926	In BIG-IP versions 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, and 14.1.0-14.1.2.6, a BIG-IP virtual server with a Session Initiation Protocol (SIP) ALG profile, parsing SIP messages that contain a multi-part MIME payload with certain boundary strings can cause TMM to free memory to the wrong cache.	7.5	More Details
CVE-2019-5645	By sending a specially crafted HTTP GET request to a listening Rapid7 Metasploit HTTP handler, an attacker can register an arbitrary regular expression. When evaluated, this malicious handler can either prevent new HTTP handler sessions from being established, or cause a resource exhaustion on the Metasploit server.	7.5	More Details
CVE-2020-7669	This affects all versions of package github.com/u-root/u-root/pkg/tarutil. It is vulnerable to both leading and non-leading relative path traversal attacks in tar file extraction.	7.5	More Details
CVE-2020-11497	An issue was discovered in the NAB Transact extension 2.1.0 for the WooCommerce plugin for WordPress. An online payment system bypass allows orders to be marked as fully paid by assigning an arbitrary bank transaction ID during the payment-details entry step.	7.5	More Details
CVE-2020-7666	This affects all versions of package github.com/u-root/u-root/pkg/cpio. It is vulnerable to leading, non-leading relative path traversal attacks and symlink based (relative and absolute) path traversal attacks in cpio file extraction.	7.5	More Details
CVE-2020-24554	The redirect module in Liferay Portal before 7.3.3 does not limit the number of URLs resulting in a 404 error that is recorded, which allows remote attackers to perform a denial of service attack by making repeated requests for pages that do not exist.	7.5	More Details
CVE-2020-24584	An issue was discovered in Django 2.2 before 2.2.16, 3.0 before 3.0.10, and 3.1 before 3.1.1 (when Python 3.7+ is used). The intermediate-level directories of the filesystem cache had the system's standard umask rather than 0o077.	7.5	More Details
CVE-2020-2075	Platform mechanism AutoIP allows remote attackers to reboot the device via a crafted packet in SICK AG solutions Bulkscan LMS111, Bulkscan LMS511, CLV62x – CLV65x, ICR890-3, LMS10x, LMS11x, LMS15x, LMS12x, LMS13x, LMS14x, LMS5xx, LMS53x, MSC800, RFH.	7.5	More Details
CVE-2019-4698	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 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: 171929.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25050	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. The CMC service allows attackers to obtain sensitive information. The Samsung ID is SVE-2020-17288 (August 2020).	7.5	More Details
CVE-2020-25051	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Attackers can bypass Factory Reset Protection (FRP) via AppInfo. The Samsung ID is SVE-2020-17758 (August 2020).	7.5	More Details
CVE-2020-25056	An issue was discovered on Samsung mobile devices with Q(10.0) (Galaxy S20) software. Because HAL improperly checks versions, bootloading by the S.LSI NFC chipset is mishandled. The Samsung ID is SVE-2020-16169 (August 2020).	7.5	More Details
CVE-2020-25059	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. A service crash may occur because of incorrect input validation. The LG ID is LVE-SMP-200013 (July 2020).	7.5	More Details
CVE-2019-4689	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 171826.	7.5	More Details
CVE-2020-25063	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. An application crash can occur because of incorrect application-level input validation. The LG ID is LVE-SMP-200018 (July 2020).	7.5	More Details
CVE-2018-1501	IBM Security Guardium 10.5, 10.6, and 11.0 could allow an unauthorized user to obtain sensitive information due to missing security controls. IBM X-Force ID: 141226.	7.5	More Details
CVE-2020-25064	An issue was discovered on LG mobile devices with Android OS 4.4, 5.0, 5.1, 6.0, 7.0, 7.1, 8.0, 8.1, 9.0, and 10 software. Certain automated testing is mishandled. The LG ID is LVE-SMP-200019 (August 2020).	7.5	More Details
CVE-2020-25065	An issue was discovered on LG mobile devices with Android OS 4.4, 5.0, 5.1, 6.0, 7.0, 7.1, 8.0, 8.1, 9.0, and 10 software. Key logging may occur because of an obsolete API. The LG ID is LVE-SMP-170010 (August 2020).	7.5	More Details
CVE-2020-14178	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to enumerate project keys via an Information Disclosure vulnerability in the /browse.PROJECTKEY endpoint. The affected versions are before version 7.13.7, from version 8.0.0 before 8.5.8, and from version 8.6.0 before 8.12.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13617	The Web UI component of Mitel MiVoice 6800 and 6900 series SIP Phones with firmware before 5.1.0.SP5 could allow an unauthenticated attacker to expose sensitive information due to improper memory handling during failed login attempts.	7.5	More Details
CVE-2020-24583	An issue was discovered in Django 2.2 before 2.2.16, 3.0 before 3.0.10, and 3.1 before 3.1.1 (when Python 3.7+ is used). FILE_UPLOAD_DIRECTORY_PERMISSIONS mode was not applied to intermediate-level directories created in the process of uploading files. It was also not applied to intermediate-level collected static directories when using the collectstatic management command.	7.5	More Details
CVE-2020-5913	In versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.2, the BIG-IP Client or Server SSL profile ignores revoked certificates, even when a valid CRL is present. This impacts SSL/TLS connections and may result in a man-in-the-middle attack on the connections.	7.4	More Details
CVE-2020-15154	baserCMS 4.3.6 and earlier is affected by Cross Site Scripting (XSS) via arbitrary script execution. Admin access is required to exploit this vulnerability. The affected components are: content_fields.php, content_info.php, content_options.php, content_related.php, index_list_tree.php, jquery.bcTree.js. The issue is fixed in version 4.3.7.	7.3	More Details
CVE-2020-15155	baserCMS 4.3.6 and earlier is affected by Cross Site Scripting (XSS) via arbitrary script execution. Admin access is required to exploit this vulnerability. The affected components is toolbar.php. The issue is fixed in version 4.3.7.	7.3	More Details
CVE-2019-14904	A flaw was found in the solaris_zone module from the Ansible Community modules. When setting the name for the zone on the Solaris host, the zone name is checked by listing the process with the 'ps' bare command on the remote machine. An attacker could take advantage of this flaw by crafting the name of the zone and executing arbitrary commands in the remote host. Ansible Engine 2.7.15, 2.8.7, and 2.9.2 as well as previous versions are affected.	7.3	More Details
CVE-2020-3454	A vulnerability in the Call Home feature of Cisco NX-OS Software could allow an authenticated, remote attacker to inject arbitrary commands that could be executed with root privileges on the underlying operating system (OS). The vulnerability is due to insufficient input validation of specific Call Home configuration parameters when the software is configured for transport method HTTP. An attacker could exploit this vulnerability by modifying parameters within the Call Home configuration on an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying OS.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8602	A vulnerability in the management consoles of Trend Micro Deep Security 10.0-12.0 and Trend Micro Vulnerability Protection 2.0 SP2 may allow an authenticated attacker with full control privileges to bypass file integrity checks, leading to remote code execution.	7.2	More Details
CVE-2020-7712	This affects the package json before 10.0.0. It is possible to inject arbritary commands using the parseLookup function.	7.2	More Details
CVE-2020-4603	IBM Security Guardium Insights 2.0.1 performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses. IBM X-Force ID: 184880.	7.2	More Details
CVE-2020-24196	An Arbitrary File Upload in Vehicle Image Upload in Online Bike Rental v1.0 allows authenticated admin to conduct remote code execution.	7.2	More Details
CVE-2020-5912	In BIG-IP versions 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, 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, the restjavad process's dump command does not follow current best coding practices and may overwrite arbitrary files.	7.1	More Details
CVE-2020-2245	Jenkins Valgrind Plugin 0.28 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	7.1	More Details
CVE-2020-24558	A vulnerability in an Trend Micro Apex One, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services dll may allow an attacker to manipulate it to cause an out-of-bounds read that crashes multiple processes in the product. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.1	More Details
CVE-2020-13465	The security protection in Gigadevice GD32F103 devices allows physical attackers to redirect the control flow and execute arbitrary code via the debug interface.	6.8	More Details
CVE-2020-15483	An issue was discovered on Nescomed Multipara Monitor M1000 devices. The physical UART debug port provides a shell, without requiring a password, with complete access.	6.8	More Details
CVE-2020-13471	Apex Microelectronics APM32F103 devices allow physical attackers to execute arbitrary code via a power glitch and a specific flash patch/breakpoint unit configuration.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5916	In BIG-IP versions 15.1.0-15.1.0.4 and 15.0.0-15.0.1.3 the Certificate Administrator user role and higher privileged roles can perform arbitrary file reads outside of the web root directory.	6.8	More Details
CVE-2020-13468	Gigadevice GD32F130 devices allow physical attackers to escalate their debug interface permissions via fault injection into inter-IC bonding wires (which have insufficient physical protection).	6.8	More Details
CVE-2020-13466	STMicroelectronics STM32F103 devices through 2020-05-20 allow physical attackers to execute arbitrary code via a power glitch and a specific flash patch/breakpoint unit configuration.	6.8	More Details
CVE-2020-15156	In nodebb-plugin-blog-comments before version 0.7.0, a logged in user is vulnerable to an XSS attack which could allow a third party to post on their behalf on the forum. This is due to lack of CSRF validation.	6.8	More Details
CVE-2020-3151	A vulnerability in the CLI of Cisco Connected Mobile Experiences (CMX) could allow an authenticated, local attacker with administrative credentials to bypass restrictions on the CLI. The vulnerability is due to insufficient security mechanisms in the restricted shell implementation. An attacker could exploit this vulnerability by sending crafted commands to the CLI. A successful exploit could allow the attacker to escape the restricted shell and execute a set of normally unauthorized commands with the privileges of a non-root user. To exploit this vulnerability, an attacker would need to have valid administrative credentials.	6.7	More Details
CVE-2020-3152	A vulnerability in Cisco Connected Mobile Experiences (CMX) could allow an authenticated, local attacker with administrative credentials to execute arbitrary commands with root privileges. The vulnerability is due to improper user permissions that are configured by default on an affected system. An attacker could exploit this vulnerability by sending crafted commands to the CLI. A successful exploit could allow the attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. To exploit this vulnerability, an attacker would need to have valid administrative credentials.	6.7	More Details
CVE-2020-5419	RabbitMQ versions 3.8.x prior to 3.8.7 are prone to a Windows-specific binary planting security vulnerability that allows for arbitrary code execution. An attacker with write privileges to the RabbitMQ installation directory and local access on Windows could carry out a local binary hijacking (planting) attack and execute arbitrary code.	6.7	More Details
CVE-2020-12776	Openfind Mail2000 contains Broken Access Control vulnerability, which can be used to execute unauthorized commands after attackers obtain the administrator access token or cookie.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3505	A vulnerability in the Cisco Discovery Protocol of Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. The vulnerability is due to incorrect processing of certain Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending certain Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DOS condition. Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	6.5	More Details
CVE-2018-12475	A Externally Controlled Reference to a Resource in Another Sphere vulnerability in obs-service-download_files of openSUSE Open Build Service allows authenticated users to generate HTTP request against internal networks and potentially downloading data that is exposed there. This issue affects: openSUSE Open Build Service .	6.5	More Details
CVE-2020-13595	The Bluetooth Low Energy (BLE) controller implementation in Espressif ESP-IDF 4.0 through 4.2 (for ESP32 devices) returns the wrong number of completed BLE packets and triggers a reachable assertion on the host stack when receiving a packet with an MIC failure. An attacker within radio range can silently trigger the assertion (which disables the target's BLE stack) by sending a crafted sequence of BLE packets.	6.5	More Details
CVE-2020-2247	Jenkins Klocwork Analysis Plugin 2020.2.1 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	6.5	More Details
CVE-2020-13594	The Bluetooth Low Energy (BLE) controller implementation in Espressif ESP-IDF 4.2 and earlier (for ESP32 devices) does not properly restrict the channel map field of the connection request packet on reception, allowing attackers in radio range to cause a denial of service (crash) via a crafted packet.	6.5	More Details
CVE-2020-3440	A vulnerability in Cisco Webex Meetings Desktop App for Windows could allow an unauthenticated, remote attacker to overwrite arbitrary files on an end-user system. The vulnerability is due to improper validation of URL parameters that are sent from a website to the affected application. An attacker could exploit this vulnerability by persuading a user to follow a URL to a website that is designed to submit crafted input to the affected application. A successful exploit could allow the attacker to overwrite arbitrary files on the affected system, possibly corrupting or deleting critical system files.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2242	A missing permission check in Jenkins database Plugin 1.6 and earlier allows attackers with Overall/Read access to Jenkins to connect to an attacker-specified database server using attacker-specified credentials.	6.5	More Details
CVE-2020-3518	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of the affected software. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. 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.	6.5	More Details
CVE-2020-15486	An issue was discovered on Dr Trust ECG Pen 2.00.08 devices. Because the Bluetooth LE support is implemented without a requirement for pairing or security, any attacker can access the GATT server of the device and can sniff the data being broadcasted while a measurement is being done. Also, saved data can also be extracted over a Bluetooth connection. In addition, an attacker can launch a man-in-the-middle attack against data integrity.	6.5	More Details
CVE-2020-3523	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, 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 persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.5	More Details
CVE-2020-8244	A buffer over-read vulnerability exists in bl <4.0.3, <3.0.1, <2.2.1, and <1.2.3 which could allow an attacker to supply user input (even typed) that if it ends up in consume() argument and can become negative, the BufferList state can be corrupted, tricking it into exposing uninitialized memory via regular .slice() calls.	6.5	More Details
CVE-2020-2250	Jenkins SoapUI Pro Functional Testing Plugin 1.3 and earlier stores project passwords unencrypted in job config.xml files on the Jenkins controller where they can be viewed by attackers with Extended Read permission, or access to the Jenkins controller file system.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4167	IBM Security Guardium Insights 2.0.1 could allow an attacker to obtain sensitive information or perform unauthorized actions due to improper authenciation mechanisms. IBM X-Force ID: 174403.	6.5	More Details
CVE-2019-19499	Grafana <= 6.4.3 has an Arbitrary File Read vulnerability, which could be exploited by an authenticated attacker that has privileges to modify the data source configurations.	6.5	More Details
CVE-2020-24656	Maltego before 4.2.12 allows XXE attacks.	6.5	More Details
CVE-2020-24618	In JetBrains YouTrack versions before 2020.3.4313, 2020.2.11008, 2020.1.11011, 2019.1.65514, 2019.2.65515, and 2019.3.65516, an attacker can retrieve an issue description without appropriate access.	6.5	More Details
CVE-2019-4697	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 stores user credentials in plain in clear text which can be read by an authenticated user. IBM X-Force ID: 171938.	6.5	More Details
CVE-2020-23835	A Reflected Cross-Site Scripting (XSS) vulnerability in the index.php login-portal webpage of SourceCodester Tailor Management System v1.0 allows remote attackers to harvest keys pressed by an unauthenticated victim who clicks on a malicious URL and begins typing.	6.4	More Details
CVE-2020-23831	A Reflected Cross-Site Scripting (XSS) vulnerability in the index.php login-portal webpage of SourceCodester Stock Management System v1.0 allows remote attackers to harvest login credentials and session cookies when an unauthenticated victim clicks on a malicious URL and enters credentials.	6.4	More Details
CVE-2020-3522	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to bypass authorization on an affected device and access sensitive information that is related to the device. The vulnerability exists because the affected software allows users to access resources that are intended for administrators only. An attacker could exploit this vulnerability by submitting a crafted URL to an affected device. A successful exploit could allow the attacker to add, delete, and edit certain network configurations in the same manner as a user with administrative privileges.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3485	A vulnerability in the role-based access control (RBAC) functionality of the web management software of Cisco Vision Dynamic Signage Director could allow an authenticated, remote attacker to access resources that they should not be able to access and perform actions that they should not be able to perform. The vulnerability exists because the web management software does not properly handle RBAC. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to view and delete certain screen content on the system that the attacker would not normally have privileges to access.	6.3	More Details
CVE-2019-5320	Aruba Intelligent Edge Switch Series 2540, 2530, 2930F, 2930M, 2920, 5400R, and 3810M with firmware 16.08.* before 16.08.0009, 16.09.* before 16.09.0007, 16.10.* before 16.10.0003 are vulnerable to Cross Site Scripting in the web UI, leading to injection of code.	6.1	More Details
CVE-2020-24223	Mara CMS 7.5 allows cross-site scripting (XSS) in contact.php via the theme or pagetheme parameters.	6.1	More Details
CVE-2020-2248	Jenkins JSGames Plugin 0.2 and earlier evaluates part of a URL as code, resulting in a reflected cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2020-24314	Fahad Mahmood RSS Feed Widget Plugin v2.7.9 and lower does not sanitize the value of the "t" GET parameter before echoing it back out inside an input tag. This results in a reflected XSS vulnerability that attackers can exploit with a specially crafted URL.	6.1	More Details
CVE-2020-24313	Etoile Web Design Ultimate Appointment Booking & Scheduling WordPress Plugin v1.1.9 and lower does not sanitize the value of the "Appointment_ID" GET parameter before echoing it back out inside an input tag. This results in a reflected XSS vulnerability that attackers can exploit with a specially crafted URL.	6.1	More Details
CVE-2020-15499	An issue was discovered on ASUS RT-AC1900P routers before 3.0.0.4.385_20253. They allow XSS via spoofed Release Notes on the Firmware Upgrade page.	6.1	More Details
CVE-2020-17465	Dashboards and progressiveProfileForms in ForgeRock Identity Manager before 7.0.0 are vulnerable to stored XSS. The vulnerability affects versions 6.5.0.4, 6.0.0.6.	6.1	More Details
CVE-2020-24917	osTicket before 1.14.3 allows XSS via a crafted filename to DraftAjaxAPI::_uploadInlineImage() in include/ajax.draft.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8335	The BIOS tamper detection mechanism was not triggered in Lenovo ThinkPad A285, BIOS versions up to r0xuj70w; A485, BIOS versions up to r0wuj65w; T495 BIOS versions up to r12uj55w; T495s/X395, BIOS versions up to r13uj47w, while the emergency-reset button is pressed which may allow for unauthorized access.	6.1	More Details
CVE-2020-24599	An issue was discovered in Joomla! before 3.9.21. Lack of escaping in mod_latestactions allows XSS attacks.	6.1	More Details
CVE-2020-24699	The Chamber Dashboard Business Directory plugin 3.2.8 for WordPress allows XSS.	6.1	More Details
CVE-2020-20628	controller/controller-comments.php in WP GDPR plugin through 2.1.1 has unauthenticated stored XSS.	6.1	More Details
CVE-2020-24598	An issue was discovered in Joomla! before 3.9.21. Lack of input validation in the vote feature of com_content leads to an open redirect.	6.1	More Details
CVE-2020-24390	eonweb in EyesOfNetwork before 5.3-7 does not properly escape the username on the /module/admin_logs page, which might allow pre-authentication stored XSS during login/logout logs recording.	6.1	More Details
CVE-2020-24704	An issue was discovered in certain WSO2 products. The Try It tool allows Reflected XSS. This affects API Manager 2.2.0, API Manager Analytics 2.2.0, API Microgateway 2.2.0, Data Analytics Server 3.2.0, Enterprise Integrator through 6.6.0, IS as Key Manager 5.5.0, Identity Server 5.5.0 and 5.8.0, Identity Server Analytics 5.5.0, and IoT Server 3.3.0 and 3.3.1.	6.1	More Details
CVE-2020-24706	An issue was discovered in certain WSO2 products. The Try It tool allows Reflected XSS. This affects API Manager through 3.1.0, API Manager Analytics 2.5.0, IS as Key Manager through 5.10.0, Identity Server through 5.10.0, Identity Server Analytics through 5.6.0, and IoT Server 3.1.0.	6.1	More Details
CVE-2020-5625	Cross-site scripting vulnerability in XooNIps 3.48 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2020-5623	NITORI App for Android versions 6.0.4 and earlier and NITORI App for iOS versions 6.0.2 and earlier allow remote attackers to lead a user to access an arbitrary website via the vulnerable App. As a result, the user may become a victim of a phishing attack.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24316	WP Plugin Rednumber Admin Menu v1.1 and lower does not sanitize the value of the "role" GET parameter before echoing it back out to the user. This results in a reflected XSS vulnerability that attackers can exploit with a specially crafted URL.	6.1	More Details
CVE-2020-23982	DesignMasterEvents Conference management 1.0.0 has cross site scripting via the 'certificate.php'	6.1	More Details
CVE-2020-23975	Webexcels Ecommerce CMS 2.x, 2017, 2018, 2019, 2020 has cross site scripting via the 'search.php' id parameter.	6.1	More Details
CVE-2020-24104	XSS on the PIX-Link Repeater/Router LV-WR07 with firmware v28K.Router.20170904 allows attackers to steal credentials without being connected to the network. The attack vector is a crafted ESSID, as demonstrated by the wireless.htm SET2 parameter.	6.1	More Details
CVE-2020-23977	KandNconcepts Club CMS 1.1 and 1.2 has cross site scripting via the 'team.php,player.php,club.php' id parameter.	6.1	More Details
CVE-2020-25033	The Blubrry subscribe-sidebar (aka Subscribe Sidebar) plugin 1.3.1 for WordPress allows subscribe_sidebar.php&status= reflected XSS.	6.1	More Details
CVE-2020-5927	In versions 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, and 14.1.0-14.1.2.6, BIG-IP ASM Configuration utility Stored-Cross Site Scripting.	6.1	More Details
CVE-2020-13655	An issue was discovered in Collabtive 3.0 and later. managefile.php is vulnerable to XSS: when the action parameter is set to movefile and the id parameter corresponds to a project the current user has access to, the file and target parameters are reflected.	6.1	More Details
CVE-2020-23981	13enforme CMS 1.0 has Cross Site Scripting via the "content.php" id parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3466	Multiple vulnerabilities in the web-based management interface of Cisco DNA Center software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. The vulnerabilities exist because the web-based management interface on an affected device does not properly validate user-supplied input. An attacker could exploit these vulnerabilities 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-2020-23839	A Reflected Cross-Site Scripting (XSS) vulnerability in GetSimple CMS v3.3.16, in the admin/index.php login portal webpage, allows remote attackers to execute JavaScript code in the client's browser and harvest login credentials after a client clicks a link, enters credentials, and submits the login form.	6.1	More Details
CVE-2020-5915	In BIG-IP versions 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, 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 undisclosed TMUI page contains a vulnerability which allows a stored XSS when BIG-IP systems are setup in a device trust.	6.1	More Details
CVE-2020-4575	IBM WebSphere Application Server ND 8.5 and 9.0, and IBM WebSphere Virtual Enterprise 7.0 and 8.0 are vulnerable to cross-site scripting when High Availability Deployment Manager is configured.	6.1	More Details
CVE-2020-5917	In BIG-IP versions 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.2 and BIG-IQ versions 5.2.0-7.0.0, the host OpenSSH servers utilize keys of less than 2048 bits which are no longer considered secure.	5.9	More Details
CVE-2020-4175	IBM Security Guardium Insights 2.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 174684.	5.9	More Details
CVE-2020-15498	An issue was discovered on ASUS RT-AC1900P routers before 3.0.0.4.385_20253. The router accepts an arbitrary server certificate for a firmware update. The culprit is the --no-check-certificate option passed to wget tool used to download firmware update files.	5.9	More Details
CVE-2020-11617	The RSS application on THOMSON THT741FTA 2.2.1 and Philips DTR3502BFTA DVB-T2 2.2.1 set-top boxes doesn't validate the SSL certificates of RSS servers, which allows a man-in-the-middle attacker to modify the data delivered to the client.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24661	GNOME Geary before 3.36.3 mishandles pinned TLS certificate verification for IMAP and SMTP services using invalid TLS certificates (e.g., self-signed certificates) when the client system is not configured to use a system-provided PKCS#11 store. This allows a meddler in the middle to present a different invalid certificate to intercept incoming and outgoing mail.	5.9	More Details
CVE-2020-13767	The Mitel MiCollab application before 9.1.332 for iOS could allow an unauthorized user to access restricted files and folders due to insufficient access control. An exploit requires a rooted iOS device, and (if successful) could allow an attacker to gain access to sensitive information,	5.9	More Details
CVE-2020-13946	In Apache Cassandra, all versions prior to 2.1.22, 2.2.18, 3.0.22, 3.11.8 and 4.0-beta2, it is possible for a local attacker without access to the Apache Cassandra process or configuration files to manipulate the RMI registry to perform a man-in-the-middle attack and capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and perform unauthorised operations. Users should also be aware of CVE-2019-2684, a JRE vulnerability that enables this issue to be exploited remotely.	5.9	More Details
CVE-2020-3520	A vulnerability in Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, local attacker to obtain confidential information from an affected device. The vulnerability is due to insufficient protection of confidential information on an affected device. An attacker at any privilege level could exploit this vulnerability by accessing local filesystems and extracting sensitive information from them. A successful exploit could allow the attacker to view sensitive data, which they could use to elevate their privilege.	5.5	More Details
CVE-2020-3491	A vulnerability in the web-based management interface of Cisco Vision Dynamic Signage Director could allow an authenticated, remote attacker with administrative privileges to conduct a cross-site scripting (XSS) attack against a user of the interface on an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in 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 this vulnerability, the attacker would need to have administrative privileges on the affected device.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25046	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The USB driver leaks address information via kernel logging. The Samsung IDs are SVE-2020-17602, SVE-2020-17603, SVE-2020-17604 (August 2020).	5.5	More Details
CVE-2020-15704	The modprobe child process in the ./debian/patches/load_ppp_generic_if_needed patch file incorrectly handled module loading. A local non-root attacker could exploit the MODPROBE_OPTIONS environment variable to read arbitrary root files. Fixed in 2.4.5-5ubuntu1.4, 2.4.5-5.1ubuntu2.3+esm2, 2.4.7-1+2ubuntu1.16.04.3, 2.4.7-2+2ubuntu1.3, 2.4.7-2+4.1ubuntu5.1, 2.4.7-2+4.1ubuntu6. Was ZDI-CAN-11504.	5.5	More Details
CVE-2020-25047	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (released in China and India) software. The S Secure application does not enforce the intended password requirement for a locked application. The Samsung IDs are SVE-2020-16746, SVE-2020-16764 (August 2020).	5.5	More Details
CVE-2020-4492	IBM Spectrum Scale V5.0.0.0 through V5.0.4.3 and V4.2.0.0 through V4.2.3.21 could allow a local attacker to cause a denial of service crashing the kernel by sending a subset of ioctls on the device with invalid arguments. IBM X-Force ID: 181992.	5.5	More Details
CVE-2020-15485	An issue was discovered on Nescomed Multipara Monitor M1000 devices. The onboard Flash memory stores data in cleartext, without integrity protection against tampering.	5.5	More Details
CVE-2020-13828	Dolibarr 11.0.4 is affected by multiple stored Cross-Site Scripting (XSS) vulnerabilities that could allow remote authenticated attackers to inject arbitrary web script or HTML via ticket/card.php?action=create with the subject, message, or address parameter; adherents/card.php with the societe or address parameter; product/card.php with the label or customcode parameter; or societe/card.php with the alias or barcode parameter.	5.4	More Details
CVE-2012-3341	IBM InfoSphere Guardium 7.0, 8.0, 8.01, and 8.2 is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials. IBM X-Force ID: 78294.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14728	Vulnerability in the SuiteCommerce Advanced (SCA) component of Oracle NetSuite service. Supported versions that are affected are Montblanc, Vinson, Elbrus, Kilimanjaro, Aconcagua, 2018.2, 2019.1, 2019.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise NetSuite SCA. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in NetSuite SCA, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of NetSuite SCA accessible data as well as unauthorized read access to a subset of NetSuite SCA data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2020-23656	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) on module "Content."	5.4	More Details
CVE-2020-23974	Create-Project Manager 1.07 has Multi Persistent Cross-site Scripting and HTML injection in via Online chat, Social feed,Message(title-tag), Add new client (all-tags).	5.4	More Details
CVE-2020-2243	Jenkins Cadence vManager Plugin 3.0.4 and earlier does not escape build descriptions in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Run/Update permission.	5.4	More Details
CVE-2020-2244	Jenkins Build Failure Analyzer Plugin 1.27.0 and earlier does not escape matching text in a form validation response, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers able to provide console output for builds used to test build log indications.	5.4	More Details
CVE-2020-2246	Jenkins Valgrind Plugin 0.28 and earlier does not escape content in Valgrind XML reports, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control Valgrind XML report contents.	5.4	More Details
CVE-2020-5923	In BIG-IP versions 15.0.0-15.1.0.4, 14.1.0-14.1.2.6, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1 and BIG-IQ versions 5.4.0-7.0.0, Self-IP port-lockdown bypass via IPv6 link-local addresses.	5.4	More Details
CVE-2020-2238	Jenkins Git Parameter Plugin 0.9.12 and earlier does not escape the repository field on the 'Build with Parameters' page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23450	Spiceworks Version <= 7.5.00107 is affected by XSS. Any name typed on Custom Groups function is vulnerable to stored XSS as they displayed on http://127.0.0.1/inventory/groups/ without output sanitization.	5.4	More Details
CVE-2020-14729	Vulnerability in SuiteCommerce Advanced (SCA) Sites component of Oracle NetSuite service. Supported versions that are affected are prior to 2020.1.4. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise NetSuite SCA. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all NetSuite SCA accessible data as well as unauthorized read access to a subset of NetSuite SCA data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:N).	5.4	More Details
CVE-2020-13821	An issue was discovered in HiveMQ Broker Control Center 4.3.2. A crafted clientid parameter in an MQTT packet (sent to the Broker) is reflected in the client section of the management console. The attacker's JavaScript is loaded in a browser, which can lead to theft of the session and cookie of the administrator's account of the Broker.	5.4	More Details
CVE-2020-12646	OX App Suite 7.10.3 and earlier allows XSS via text/x-javascript, text/rdf, or a PDF document.	5.4	More Details
CVE-2020-15020	An issue was discovered in the Elementor plugin through 2.9.13 for WordPress. An authenticated attacker can achieve stored XSS via the Name Your Template field.	5.4	More Details
CVE-2020-23654	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) via the module "Shop."	5.4	More Details
CVE-2020-23655	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) on module "Configuration."	5.4	More Details
CVE-2020-23983	Michael-design iChat Realtime PHP Live Support System 1.6 has persistent Cross-site Scripting via chat,text-filed tags.	5.4	More Details
CVE-2020-23657	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) on module "Configuration."	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20626	lara-google-analytics.php in Lara Google Analytics plugin through 2.0.4 for WordPress allows authenticated stored XSS.	5.4	More Details
CVE-2020-16193	osTicket before 1.14.3 allows XSS because include/staff/banrule.inc.php has an unvalidated echo $info['notes'] call.	5.4	More Details
CVE-2020-23576	Laborator Neon dashboard v3 is affected by stored Cross Site Scripting (XSS) via the chat tab.	5.4	More Details
CVE-2020-23658	PHP-Fusion 9.03.60 is affected by Cross Site Scripting (XSS) via infusions/member_poll_panel/poll_admin.php.	5.4	More Details
CVE-2020-19007	Halo blog 1.2.0 allows users to submit comments on blog posts via /api/content/posts/comments. The javascript code supplied by the attacker will then execute in the victim user's browser.	5.4	More Details
CVE-2020-23659	WebPort-v1.19.17121 is affected by Cross Site Scripting (XSS) on the "connections" feature.	5.4	More Details
CVE-2020-23660	webTareas v2.1 is affected by Cross Site Scripting (XSS) on "Search."	5.4	More Details
CVE-2019-4691	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 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: 171828.	5.4	More Details
CVE-2020-23984	Online Hotel Booking System Pro PHP Version 1.3 has Persistent Cross-site Scripting in Customer registration-form all-tags.	5.4	More Details
CVE-2020-3521	A vulnerability in a specific REST API of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. The vulnerability is due to insufficient validation of user-supplied input to the API. An attacker with a low-privileged account could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to read arbitrary files on the affected system.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5383	Dell EMC Isilon OneFS version 8.2.2 and Dell EMC PowerScale OneFS version 9.0.0 contains a buffer overflow vulnerability in the Likewise component. A remote unauthenticated malicious attacker may potentially exploit this vulnerability to cause a process restart.	5.3	More Details
CVE-2020-4166	IBM Security Guardium Insights 2.0.1 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: 174402.	5.3	More Details
CVE-2019-4701	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 171936.	5.3	More Details
CVE-2019-4692	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 171829.	5.3	More Details
CVE-2020-3484	A vulnerability in the web-based management interface of Cisco Vision Dynamic Signage Director could allow an unauthenticated, remote attacker to view potentially sensitive information on an affected device. The vulnerability is due to incorrect permissions within Apache configuration. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface. A successful exploit could allow the attacker to view potentially sensitive information on the affected device.	5.3	More Details
CVE-2020-4172	IBM Security Guardium Insights 2.0.1 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 174408.	5.3	More Details
CVE-2020-5924	In BIG-IP APM versions 12.1.0-12.1.5.1 and 11.6.1-11.6.5.2, RADIUS authentication leaks memory when the username for authentication is not set.	5.3	More Details
CVE-2019-4686	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 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: 171822.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3496	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause the switch management CLI to stop responding, resulting in a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	5.3	More Details
CVE-2012-3337	IBM InfoSphere Guardium 8.0, 8.01, and 8.2 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to download arbitrary files on the system. IBM X-Force ID: 78284.	5.3	More Details
CVE-2012-3338	IBM InfoSphere Guardium 8.0, 8.01, and 8.2 could allow a remote attacker to bypass security restrictions, caused by improper restrictions on the create new user account functionality. An attacker could exploit this vulnerability to create unprivileged user accounts. IBM X-Force ID: 78286.	5.3	More Details
CVE-2020-24928	managers/socketManager.ts in PreMiD through 2.1.3 has a locally hosted socketio web server (port 3020) open to all origins, which allows attackers to obtain sensitive Discord user information.	5.3	More Details
CVE-2020-24548	Ericom Access Server 9.2.0 (for AccessNow and Ericom Blaze) allows SSRF to make outbound WebSocket connection requests on arbitrary TCP ports, and provides "Cannot connect to" error messages to inform the attacker about closed ports.	5.3	More Details
CVE-2020-24008	Umanni RH 1.0 has a user enumeration vulnerability. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	5.3	More Details
CVE-2020-20627	The includes/gateways/stripe/includes/admin/admin-actions.php in GiveWP plugin through 2.5.9 for WordPress allows unauthenticated settings change.	5.3	More Details
CVE-2020-6873	A ZTE product has a DoS vulnerability. Because the equipment couldn’t distinguish the attack packets and normal packets with valid http links, the remote attackers could use this vulnerability to cause the equipment WEB/TELNET module denial of service and make the equipment be out of management. This affects: ZXR10 2800-4_ALMPUFB(LOW), all versions up to V3.00.40.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12644	OX App Suite 7.10.3 and earlier allows SSRF, related to the mail account API and the /folder/list API.	5.0	More Details
CVE-2020-14364	An out-of-bounds read/write access flaw was found in the USB emulator of the QEMU in versions before 5.2.0. This issue occurs while processing USB packets from a guest when USBDevice 'setup_len' exceeds its 'data_buf[4096]' in the do_token_in, do_token_out routines. This flaw allows a guest user to crash the QEMU process, resulting in a denial of service, or the potential execution of arbitrary code with the privileges of the QEMU process on the host.	5.0	More Details
CVE-2020-3490	A vulnerability in the web-based management interface of Cisco Vision Dynamic Signage Director could allow an authenticated, remote attacker with administrative privileges to conduct directory traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to read files on the underlying operating system with root privileges. To exploit this vulnerability, the attacker would need to have administrative privileges on the affected system.	4.9	More Details
CVE-2020-3439	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. 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.	4.8	More Details
CVE-2020-13463	The flash memory readout protection in Apex Microelectronics APM32F103 devices allows physical attackers to extract firmware via the debug interface and exception handling.	4.6	More Details
CVE-2020-25048	An issue was discovered on Samsung mobile devices with Q(10.0) (with ONEUI 2.1) software. In the Lockscreen state, the Quick Share feature allows unauthenticated downloads, aka file injection. The Samsung ID is SVE-2020-17760 (August 2020).	4.6	More Details
CVE-2020-13470	Gigadevice GD32F103 and GD32F130 devices allow physical attackers to extract data via the probing of easily accessible bonding wires and de-obfuscation of the observed data.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13469	The flash memory readout protection in Gigadevice GD32VF103 devices allows physical attackers to extract firmware via the debug interface by utilizing the CPU.	4.6	More Details
CVE-2020-13467	The flash memory readout protection in China Key Systems & Integrated Circuit CKS32F103 devices allows physical attackers to extract firmware via the debug interface and exception handling.	4.6	More Details
CVE-2020-13472	The flash memory readout protection in Gigadevice GD32F103 devices allows physical attackers to extract firmware via the debug interface by utilizing the DMA module.	4.6	More Details
CVE-2019-4693	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 stores user credentials in plain in clear text which can be read by a local privileged user. IBM X-Force ID: 171831.	4.4	More Details
CVE-2020-3389	A vulnerability in the installation component of Cisco Hyperflex HX-Series Software could allow an authenticated, local attacker to retrieve the password that was configured at installation on an affected device. The vulnerability exists because sensitive information is stored as clear text. An attacker could exploit this vulnerability by authenticating to an affected device and navigating to the directory that contains sensitive information. A successful exploit could allow the attacker to obtain sensitive information in clear text from the affected device.	4.4	More Details
CVE-2020-2251	Jenkins SoapUI Pro Functional Testing Plugin 1.5 and earlier transmits project passwords in its configuration in plain text as part of job configuration forms, potentially resulting in their exposure.	4.3	More Details
CVE-2020-16610	Hoosk Codeigniter CMS before 1.7.2 is affected by a Cross Site Request Forgery (CSRF). When an attacker induces authenticated admin user to a malicious web page, any accounts can be deleted without admin user's intention.	4.3	More Details
CVE-2020-10517	An improper access control vulnerability was identified in GitHub Enterprise Server that allowed authenticated users of the instance to determine the names of unauthorized private repositories given their numerical IDs. This vulnerability did not allow unauthorized access to any repository content besides the name. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22 and was fixed in versions 2.21.6, 2.20.15, and 2.19.21. This vulnerability was reported via the GitHub Bug Bounty program.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5621	Cross-site request forgery (CSRF) vulnerability in NETGEAR switching hubs (GS716Tv2 Firmware version 5.4.2.30 and earlier, and GS724Tv3 Firmware version 5.4.2.30 and earlier) allow remote attackers to hijack the authentication of administrators and alter the settings of the device via unspecified vectors.	4.3	More Details
CVE-2019-4688	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 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: 171825.	4.3	More Details
CVE-2019-4533	IBM Resilient SOAR V38.0 users may experience a denial of service of the SOAR Platform due to a insufficient input validation. IBM X-Force ID: 165589.	4.3	More Details
CVE-2019-4579	IBM Resilient SOAR 38 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 167236.	4.3	More Details
CVE-2020-14514	All trailer Power Line Communications are affected. PLC bus traffic can be sniffed reliably via an active antenna up to 6 feet away. Further distances are also possible, subject to environmental conditions and receiver improvements.	4.3	More Details
CVE-2020-12643	OX App Suite 7.10.3 and earlier has Incorrect Access Control via an /api/subscriptions request for a snippet containing an email address.	4.3	More Details
CVE-2020-2239	Jenkins Parameterized Remote Trigger Plugin 3.1.3 and earlier stores a secret unencrypted in its global configuration file on the Jenkins controller where it can be viewed by attackers with access to the Jenkins controller file system.	4.3	More Details
CVE-2020-5920	In versions 15.0.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, a vulnerability in the BIG-IP AFM Configuration utility may allow any authenticated BIG-IP user to perform a read-only blind SQL injection attack.	4.3	More Details
CVE-2020-4171	IBM Security Guardium Insights 2.0.1 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 174407.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2012-3340	IBM InfoSphere Guardium 8.0, 8.01, and 8.2 is vulnerable to XML external entity injection, caused by improper validation of user-supplied input. A remote authenticated attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 78291.	4.3	More Details
CVE-2020-13464	The flash memory readout protection in China Key Systems & Integrated Circuit CKS32F103 devices allows physical attackers to extract firmware via the debug interface by utilizing the CPU or DMA module.	4.2	More Details
CVE-2020-7309	Cross Site Scripting vulnerability in ePO extension in McAfee Application Control (MAC) prior to 8.3.1 allows administrators to inject arbitrary web script or HTML via specially crafted input in the policy discovery section.	3.9	More Details
CVE-2020-12829	In QEMU through 5.0.0, an integer overflow was found in the SM501 display driver implementation. This flaw occurs in the COPY_AREA macro while handling MMIO write operations through the sm501_2d_engine_write() callback. A local attacker could abuse this flaw to crash the QEMU process in sm501_2d_operation() in hw/display/sm501.c on the host, resulting in a denial of service.	3.8	More Details
CVE-2020-16142	On Mercedes-Benz C Class AMG Premium Plus c220 BlueTec vehicles, the Bluetooth stack mishandles %x and %c format-string specifiers in a device name in the COMAND infotainment software.	3.5	More Details
CVE-2019-4695	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 171926.	3.3	More Details
CVE-2020-3504	A vulnerability in the local management (local-mgmt) CLI of Cisco UCS Manager Software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper handling of CLI command parameters. An attacker could exploit this vulnerability by executing specific commands on the local-mgmt CLI on an affected device. A successful exploit could allow the attacker to cause internal system processes to fail to terminate properly, which could result in a buildup of stuck processes and lead to slowness in accessing the UCS Manager CLI and web UI. A sustained attack may result in a restart of internal UCS Manager processes and a temporary loss of access to the UCS Manager CLI and web UI.	3.3	More Details
CVE-2020-14415	oss_write in audio/ossaudio.c in QEMU before 5.0.0 mishandles a buffer position.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2249	Jenkins Team Foundation Server Plugin 5.157.1 and earlier stores a webhook secret unencrypted in its global configuration file on the Jenkins controller where it can be viewed by attackers with access to the Jenkins controller file system.	3.3	More Details
CVE-2020-4591	IBM Spectrum Protect Server 8.1.0.000 through 8.1.10.000 could disclose sensitive information in nondefault settings due to occasionally not encrypting the second chunk of an object in an encrypted container pool. IBM X-Force ID: 184746.	3.3	More Details
CVE-2020-5928	In versions 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, 14.1.0-14.1.2.6, 13.1.0-13.1.3.4, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, BIG-IP ASM Configuration utility CSRF protection token can be reused multiple times.	3.1	More Details
CVE-2019-4699	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 generates an error message that includes sensitive information about its environment, users, or associated data. IBM X-Force ID: 171931.	2.7	More Details
CVE-2020-8341	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). After resuming from S3 sleep mode in various versions of BIOS for some Lenovo ThinkPad systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected.	2.4	More Details
CVE-2019-18392	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details