SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 14 October 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-2020-13957	Apache Solr versions 6.6.0 to 6.6.6, 7.0.0 to 7.7.3 and 8.0.0 to 8.6.2 prevents some features considered dangerous (which could be used for remote code execution) to be configured in a ConfigSet that's uploaded via API without authentication/authorization. The checks in place to prevent such features can be circumvented by using a combination of UPLOAD/CREATE actions.	9.8	More Details
CVE-2020-11800	Zabbix Server 2.2.x and 3.0.x before 3.0.31, and 3.2 allows remote attackers to execute arbitrary code.	9.8	More Details
CVE-2020-25273	In SourceCodester Online Bus Booking System 1.0, there is Authentication bypass on the Admin Login screen in admin.php via username or password SQL injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1914	A logic vulnerability when handling the SaveGeneratorLong instruction in Facebook Hermes prior to commit b2021df620824627f5a8c96615edbd1eb7fdddfc allows attackers to potentially read out of bounds or theoretically execute arbitrary code via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected.	9.8	More Details
CVE-2020-17407	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Microhard Bullet-LTE prior to v1.2.0-r1112. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of authentication headers. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-10596.	9.8	More Details
CVE-2019-17444	Jfrog Artifactory uses default passwords (such as "password") for administrative accounts and does not require users to change them. This may allow unauthorized network-based attackers to completely compromise of Jfrog Artifactory. This issue affects Jfrog Artifactory versions prior to 6.17.0.	9.8	More Details
CVE-2020-26867	ARC Informatique PcVue prior to version 12.0.17 is vulnerable due to the deserialization of untrusted data, which may allow an attacker to remotely execute arbitrary code on the web and mobile back-end server.	9.8	More Details
CVE-2020-5135	A buffer overflow vulnerability in SonicOS allows a remote attacker to cause Denial of Service (DoS) and potentially execute arbitrary code by sending a malicious request to the firewall. This vulnerability affected SonicOS Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version 7.0.0.0.	9.8	More Details
CVE-2020-26948	Emby Server before 4.5.0 allows SSRF via the Items/RemoteSearch/Image ImageURL parameter.	9.8	More Details
CVE-2020-26935	An issue was discovered in SearchController in phpMyAdmin before 4.9.6 and 5.x before 5.0.3. A SQL injection vulnerability was discovered in how phpMyAdmin processes SQL statements in the search feature. An attacker could use this flaw to inject malicious SQL in to a query.	9.8	More Details
CVE-2020-26919	NETGEAR JGS516PE devices before 2.6.0.43 are affected by lack of access control at the function level.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26928	Certain NETGEAR devices are affected by authentication bypass. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.	9.6	More Details
CVE-2020-26926	Certain NETGEAR devices are affected by authentication bypass. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.	9.6	More Details
CVE-2020-26907	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	9.6	More Details
CVE-2020-26906	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.	9.6	More Details
CVE-2020-26905	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.	9.6	More Details
CVE-2020-26904	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.	9.6	More Details
CVE-2020-26903	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.	9.6	More Details
CVE-2020-26902	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26901	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	9.6	More Details
CVE-2020-26900	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	9.6	More Details
CVE-2020-26899	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.	9.6	More Details
CVE-2020-26898	NETGEAR RAX40 devices before 1.0.3.80 are affected by incorrect configuration of security settings.	9.6	More Details
CVE-2020-26897	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.	9.6	More Details
CVE-2020-26908	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.00.36, D7000 before 1.0.1.74, PR2000 before 1.0.0.30, R6020 before 1.0.0.42, R6050 before 1.0.1.22, JR6150 before 1.0.1.22, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6260 before 1.1.0.64, R6700v2 before 1.2.0.62, R6800 before 1.2.0.62, R69002 before 1.2.0.62, and WNR2020 before 1.1.0.62.	9.4	More Details
CVE-2020-26927	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.00.40, D7000 before 1.0.1.78, R6020 before 1.0.0.42, R6080 before 1.0.0.42, R6050 before 1.0.1.26, JR6150 before 1.0.1.26, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.66, R6700v2 before 1.2.0.62, R6800 before 1.2.0.62, R6900v2 before 1.2.0.62, AC2100 before 1.2.0.62, AC2400 before 1.2.0.62, AC2600 before 1.2.0.62, R7450 before 1.2.0.62, and WNR2020 before 1.1.0.62.	9.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15243	Affected versions of Smartstore have a missing WebApi Authentication attribute. This vulnerability affects Smartstore shops in version 4.0.0 & 4.0.1 which have installed and activated the Web API plugin. Users of Smartstore 4.0.0 and 4.0.1 must merge their repository with 4.0.x or overwrite the file SmartStore.Web.Framework in the */bin* directory of the deployed shop with this file. As a workaround without updating uninstall the Web API plugin to close this vulnerability.	9.1	More Details
CVE-2020-13347	A command injection vulnerability was discovered in Gitlab runner versions prior to 13.2.4, 13.3.2 and 13.4.1. When the runner is configured on a Windows system with a docker executor, which allows the attacker to run arbitrary commands on Windows host, via DOCKER_AUTH_CONFIG build variable.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-26920	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.3.110, SRR60 before 2.5.3.110, and SRS60 before 2.5.3.110.	8.8	More Details
CVE-2020-26596	The Dynamic OOO widget for the Elementor Pro plugin through 3.0.5 for WordPress allows remote authenticated users to execute arbitrary code because only the Editor role is needed to upload executable PHP code via the PHP Raw snippet. NOTE: this issue can be mitigated by removing the Dynamic OOO widget or by restricting availability of the Editor role.	8.8	More Details
CVE-2020-4280	IBM QRadar SIEM 7.3 and 7.4 could allow a remote attacker to execute arbitrary commands on the system, caused by insecure deserialization of user-supplied content by the Java deserialization function. By sending a malicious serialized Java object, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 176140.	8.8	More Details
CVE-2020-26802	forma.lms 2.3.0.2 is affected by Cross Site Request Forgery (CSRF) in formalms/appCore/index.php?r=lms/profile/show&ap=saveinfo via a GET request to change the admin email address in order to accomplish an account takeover.	8.8	More Details
CVE-2020-2286	Jenkins Role-based Authorization Strategy Plugin 3.0 and earlier does not properly invalidate a permission cache when the configuration is changed, resulting in permissions being granted based on an outdated configuration.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15838	The Agent Update System in ConnectWise Automate before 2020.8 allows Privilege Escalation because the _LTUPDATE folder has weak permissions.	8.8	More Details
CVE-2020-26522	A cross-site request forgery (CSRF) vulnerability in mod/user/act_user.php in Garfield Petshop through 2020-10-01 allows remote attackers to hijack the authentication of administrators for requests that create new administrative accounts.	8.8	More Details
CVE-2020-26909	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D7800 before 1.0.1.58 and R7500v2 before 1.0.3.48.	8.8	More Details
CVE-2020-3544	A vulnerability in the Cisco Discovery Protocol implementation for Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute arbitrary code on an affected device or cause the device to reload. This vulnerability is due to missing checks when an IP camera processes a Cisco Discovery Protocol packet. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. 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 this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	8.8	More Details
CVE-2020-17406	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Microhard Bullet-LTE prior to v1.2.0-r1112. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of the ping parameter provided to tools.sh. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-10595.	8.8	More Details
CVE-2020-15176	In GLPI before version 9.5.2, when supplying a back tick in input that gets put into a SQL query,the application does not escape or sanitize allowing for SQL Injection to occur. Leveraging this vulnerability an attacker is able to exfiltrate sensitive information like passwords, reset tokens, personal details, and more. The issue is patched in version 9.5.2	8.7	More Details
CVE-2020-13340	An issue has been discovered in GitLab affecting all versions prior to 13.2.10, 13.3.7 and 13.4.2: Stored XSS in CI Job Log	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15012	A Directory Traversal issue was discovered in Sonatype Nexus Repository Manager 2.x before 2.14.19. A user that requests a crafted path can traverse up the file system to get access to content on disk (that the user running nxrm also has access to).	8.6	More Details
CVE-2020-26910	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.4	More Details
CVE-2020-26911	Certain NETGEAR devices are affected by lack of access control at the function level. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JR6150 before 1.0.1.24, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.64, R6700v2 before 1.2.0.62, R6800 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.62, and WNR2020 before 1.1.0.62.	8.3	More Details
CVE-2020-26921	Certain NETGEAR devices are affected by authentication bypass. This affects GS110EMX before 1.0.1.7, GS810EMX before 1.7.1.3, XS512EM before 1.0.1.3, and XS724EM before 1.0.1.3.	8.3	More Details
CVE-2020-4388	IBM Cognos Analytics 11.0 and 11.1 could be vulnerable to a denial of service attack by failing to catch exceptions in a servlet also exposing debug information could also be used in future attacks. IBM X-Force ID: 179270.	8.2	More Details
CVE-2020-26945	MyBatis before 3.5.6 mishandles deserialization of object streams.	8.1	More Details
CVE-2020-4779	A HTTP Verb Tampering vulnerability may impact IBM Curam Social Program Management 7.0.9 and 7.0.10. By sending a specially-crafted request, an attacker could exploit this vulnerability to bypass security access controls. IBM X-Force ID: 189156.	8.1	More Details
CVE-2020-25985	MonoCMS Blog 1.0 is affected by: Arbitrary File Deletion. Any authenticated user can delete files on and off the webserver (php files can be unlinked and not deleted).	8.1	More Details
CVE-2020-4772	An XML External Entity Injection (XXE) vulnerability may impact IBM Curam Social Program Management 7.0.9 and 7.0.10. A remote attacker could exploit this vulnerability to expose sensitive information, denial of service, server side request forgery or consume memory resources. IBM X-Force ID: 189150.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15177	In GLPI before version 9.5.2, the `install/install.php` endpoint insecurely stores user input into the database as `url_base` and `url_base_api`. These settings are referenced throughout the application and allow for vulnerabilities like Cross-Site Scripting and Insecure Redirection Since authentication is not required to perform these changes,anyone could point these fields at malicious websites or form input in a way to trigger XSS. Leveraging JavaScript it's possible to steal cookies, perform actions as the user, etc. The issue is patched in version 9.5.2.	8.0	More Details
CVE-2020-17412	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.0.0.35798. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11224.	7.8	More Details
CVE-2020-26947	monero-wallet-gui in Monero GUI before 0.17.1.0 includes the . directory in an embedded RPATH (with a preference ahead of /usr/lib), which allows local users to gain privileges via a Trojan horse library in the current working directory.	7.8	More Details
CVE-2020-17416	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.0.0.35798. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11497.	7.8	More Details
CVE-2020-17417	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.0.1.35811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11657.	7.8	More Details
CVE-2019-19115	An escalation of privilege vulnerability in Nahimic APO Software Component Driver 1.4.2, 1.5.0, 1.5.1, 1.6.1 and 1.6.2 allows an attacker to execute code with SYSTEM privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26894	LiveCode v9.6.1 on Windows allows local, low-privileged users to gain privileges by creating a malicious "cmd.exe" in the folder of the vulnerable LiveCode application. If the application is using LiveCode's "shell()" function, it will attempt to search for "cmd.exe" in the folder of the current application and run the malicious "cmd.exe".	7.8	More Details
CVE-2020-4799	IBM Informix spatial 14.10 could allow a local user to execute commands as a privileged user due to an out of bounds write vulnerability. IBM X-Force ID: 189460.	7.8	More Details
CVE-2020-12928	A vulnerability in a dynamically loaded AMD driver in AMD Ryzen Master V15 may allow any authenticated user to escalate privileges to NT authority system.	7.8	More Details
CVE-2020-17410	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.0.0.35798. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of GIF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11135.	7.8	More Details
CVE-2020-17415	This vulnerability allows local attackers to escalate privileges on affected installations of Foxit PhantomPDF 10.0.0.35798. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of the configuration files used by the Foxit PhantomPDF Update Service. The issue results from incorrect permissions set on a resource used by the service. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of SYSTEM. Was ZDI-CAN-11308.	7.8	More Details
CVE-2020-3535	A vulnerability in the loading mechanism of specific DLLs in the Cisco Webex Teams client for Windows could allow an authenticated, local attacker to load a malicious library. To exploit this vulnerability, the attacker needs valid credentials on the Windows system. The vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file in a specific location on the targeted system. This file will execute when the vulnerable application launches. A successful exploit could allow the attacker to execute arbitrary code on the targeted system with the privileges of another user’s account.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9090	FusionAccess version 6.5.1 has an improper authorization vulnerability. A command is authorized with incorrect privilege. Attackers with other privilege can execute the command to exploit this vulnerability. This may compromise normal service of the affected product.	7.8	More Details
CVE-2020-17413	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.0.0.35798. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11226.	7.8	More Details
CVE-2020-26880	Sympa through 6.2.57b.2 allows a local privilege escalation from the sympa user account to full root access by modifying the sympa.conf configuration file (which is owned by sympa) and parsing it through the setuid sympa_newaliases-wrapper executable.	7.8	More Details
CVE-2020-17414	This vulnerability allows local attackers to escalate privileges on affected installations of Foxit Reader 10.0.0.35798. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of the configuration files used by the Foxit Reader Update Service. The issue results from incorrect permissions set on a resource used by the service. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of SYSTEM. Was ZDI-CAN-11229.	7.8	More Details
CVE-2020-9123	HUAWEI P30 Pro versions earlier than 10.1.0.160(C00E160R2P8) and versions earlier than 10.1.0.160(C01E160R2P8) have a buffer overflow vulnerability. An attacker induces users to install malicious applications and sends specially constructed packets to affected devices after obtaining the root permission. Successful exploit may cause code execution.	7.8	More Details
CVE-2020-4302	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to execute arbitrary code on the system, caused by a CSV injection. By persuading a victim to open a specially-crafted excel file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 176610.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15251	In the ChannelMgnt plug-in for Sopel (a Python IRC bot) before version 1.0.3, malicious users are able to op/voice and take over a channel. This is an ACL bypass vulnerability. This plugin is bundled with MirahezeBot-Plugins with versions from 9.0.0 and less than 9.0.2 affected. Version 9.0.2 includes 1.0.3 of channelmgnt, and thus is safe from this vulnerability. See referenced GHSA-23pc-4339-95vg.	7.7	More Details
CVE-2020-3467	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to modify parts of the configuration on an affected device. The vulnerability is due to improper enforcement of role-based access control (RBAC) within the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to modify parts of the configuration. The modified configuration could either allow unauthorized devices onto the network or prevent authorized devices from accessing the network. To exploit this vulnerability, an attacker would need valid Read-Only Administrator credentials.	7.7	More Details
CVE-2019-4545	IBM QRadar SIEM 7.3 and 7.4 when configured to use Active Directory Authentication may be susceptible to spoofing attacks. IBM X-Force ID: 165877.	7.5	More Details
CVE-2020-5139	A vulnerability in SonicOS SSLVPN service allows a remote unauthenticated attacker to cause Denial of Service (DoS) due to the release of Invalid pointer and leads to a firewall crash. This vulnerability affected SonicOS Gen 5 version 5.9.1.7, 5.9.1.13, Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version SonicOS 7.0.0.0.	7.5	More Details
CVE-2020-10816	Zoho ManageEngine Applications Manager 14780 and before allows a remote unauthenticated attacker to register managed servers via AAMRequestProcessor servlet.	7.5	More Details
CVE-2020-25645	A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel allowing anyone between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.	7.5	More Details
CVE-2020-26546	An issue was discovered in HelpDeskZ 1.0.2. The feature to auto-login a user, via the RememberMe functionality, is prone to SQL injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5138	A Heap Overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS) on the firewall SSLVPN service and leads to SonicOS crash. This vulnerability affected SonicOS Gen 5 version 5.9.1.7, 5.9.1.13, Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version SonicOS 7.0.0.0.	7.5	More Details
CVE-2018-20243	The implementation of POST with the username and password in the URL parameters exposed the credentials. More infomration is available in fineract jira issues 726 and 629.	7.5	More Details
CVE-2020-4776	A path traversal vulnerability may impact IBM Curam Social Program Management 7.0.9 and 7.0.10, which could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted file path in URL request to view arbitrary files on the system. IBM X-Force ID: 189154.	7.5	More Details
CVE-2020-25825	In Octopus Deploy 3.1.0 to 2020.4.0, certain scripts can reveal sensitive information to the user in the task logs.	7.5	More Details
CVE-2020-5137	A buffer overflow vulnerability in SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS) on the firewall SSLVPN service and leads to firewall crash. This vulnerability affected SonicOS Gen 5 version 5.9.1.7, 5.9.1.13, Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version 7.0.0.0.	7.5	More Details
CVE-2020-5133	A vulnerability in SonicOS allows a remote unauthenticated attacker to cause Denial of Service due to buffer overflow, which leads to a firewall crash. This vulnerability affected SonicOS Gen 6 version 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version 7.0.0.0.	7.5	More Details
CVE-2020-5140	A vulnerability in SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS) on the firewall SSLVPN service by sending a malicious HTTP request that leads to memory addresses leak. This vulnerability affected SonicOS Gen 5 version 5.9.1.7, 5.9.1.13, Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version SonicOS 7.0.0.0.	7.5	More Details
CVE-2020-26912	Certain NETGEAR devices are affected by CSRF. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JR6150 before 1.0.1.24, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.64, R6700v2 before 1.2.0.62, R6800 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.62, and WNR2020 before 1.1.0.62.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26869	ARC Informatique PcVue prior to version 12.0.17 is vulnerable to information exposure, allowing unauthorized users to access session data of legitimate users. This issue also affects third-party systems based on the Web Services Toolkit.	7.5	More Details
CVE-2020-26868	ARC Informatique PcVue prior to version 12.0.17 is vulnerable to a denial-of-service attack due to the ability of an unauthorized user to modify information used to validate messages sent by legitimate web clients. This issue also affects third-party systems based on the Web Services Toolkit.	7.5	More Details
CVE-2020-4778	IBM Curam Social Program Management 7.0.9 and 7.0.10 uses MD5 algorithm for hashing token in a single instance which less safe than default SHA-256 cryptographic algorithm used throughout the CÃºram application. IBM X-Force ID: 189156.	7.5	More Details
CVE-2020-7742	This affects the package simpl-schema before 1.10.2.	7.5	More Details
CVE-2019-16160	An integer underflow in the SMB server of MikroTik RouterOS before 6.45.5 allows remote unauthenticated attackers to crash the service.	7.5	More Details
CVE-2020-26876	The wp-courses plugin through 2.0.27 for WordPress allows remote attackers to bypass the intended payment step (for course videos and materials) by using the /wp-json REST API, as exploited in the wild in September 2020. This occurs because show_in_rest is enabled for custom post types (e.g., /wp-json/wp/v2/course and /wp-json/wp/v2/lesson exist).	7.5	More Details
CVE-2020-24246	Peplink Balance before 8.1.0rc1 allows an unauthenticated attacker to download PHP configuration files (/filemanager/php/connector.php) from Web Admin.	7.5	More Details
CVE-2020-15175	In GLPI before version 9.5.2, the `pluginimage.send.php` endpoint allows a user to specify an image from a plugin. The parameters can be maliciously crafted to instead delete the .htaccess file for the files directory. Any user becomes able to read all the files and folders contained in “/files/”. Some of the sensitive information that is compromised are the user sessions, logs, and more. An attacker would be able to get the Administrators session token and use that to authenticate. The issue is patched in version 9.5.2.	7.4	More Details
CVE-2020-26929	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6220 before 1.1.0.100 and R6230 before 1.1.0.100.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7743	The package mathjs before 7.5.1 are vulnerable to Prototype Pollution via the deepExtend function that runs upon configuration updates.	7.3	More Details
CVE-2020-16124	Integer Overflow or Wraparound vulnerability in the XML RPC library of OpenRobotics ros_comm communications packages allows unauthenticated network traffic to cause unexpected behavior. This issue affects: OpenRobotics ros_comm communications packages Noetic and prior versions. Fixed in https://github.com/ros/ros_comm/pull/2065.	7.3	More Details
CVE-2020-9048	A vulnerability in specified versions of American Dynamics victor Web Client and Software House CCURE Web Client could allow a remote unauthenticated attacker on the network to delete arbitrary files on the system or render the system unusable by conducting a Denial of Service attack.	7.1	More Details
CVE-2020-25263	PyroCMS 3.7 is vulnerable to cross-site request forgery (CSRF) via the admin/addons/uninstall/anomaly.module.blocks URI: an arbitrary plugin will be deleted.	7.1	More Details
CVE-2020-15797	A vulnerability has been identified in DCA Vantage Analyzer (All versions < V4.5 are affected by CVE-2020-7590. In addition, serial numbers < 40000 running software V4.4.0 are also affected by CVE-2020-15797). Improper Access Control could allow an unauthenticated attacker to escape from the restricted environment (“kiosk mode”) and access the underlying operating system. Successful exploitation requires direct physical access to the system.	6.8	More Details
CVE-2020-7590	A vulnerability has been identified in DCA Vantage Analyzer (All versions < V4.5 are affected by CVE-2020-7590. In addition, serial numbers < 40000 running software V4.4.0 are also affected by CVE-2020-15797). Affected devices use a hard-coded password to protect the onboard database. This could allow an attacker to read and or modify the onboard database. Successful exploitation requires direct physical access to the device.	6.8	More Details
CVE-2020-26913	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.63, R7800 before 1.0.2.60, R8900 before 1.0.4.26, R9000 before 1.0.4.26, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, RBS50 before 2.3.0.32, RBK40 before 2.3.0.28, RBR40 before 2.3.0.28, RBS40 before 2.3.0.28, SRK60 before 2.2.2.20, SRR60 before 2.2.2.20, SRS60 before 2.2.2.20, WN3000RPv2 before 1.0.0.78, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, WNR2000v5 before 1.0.0.70, XR450 before 2.3.2.40, and XR500 before 2.3.2.40.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4689	IBM Security Guardium 11.2 is vulnerable to CVS Injection. A remote privileged attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-ForceID: 186696.	6.8	More Details
CVE-2020-9105	Taurus-AN00B versions earlier than 10.1.0.156(C00E155R7P2) have an insufficient input validation vulnerability. Due to the input validation logic is incorrect, an attacker can exploit this vulnerability to access and modify the memory of the device by doing a series of operations. Successful exploit may cause the service abnormal.	6.7	More Details
CVE-2020-26914	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JR6150 before 1.0.1.24, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.64, R6700v2 before 1.2.0.62, R6800 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.62, and WNR2020 before 1.1.0.62.	6.7	More Details
CVE-2020-7316	Unquoted service path vulnerability in McAfee File and Removable Media Protection (FRP) prior to 5.3.0 allows local users to execute arbitrary code, with higher privileges, via execution and from a compromised folder. This issue may result in files not being encrypted when a policy is triggered.	6.6	More Details
CVE-2020-14355	Multiple buffer overflow vulnerabilities were found in the QUIC image decoding process of the SPICE remote display system, before spice-0.14.2-1. Both the SPICE client (spice-gtk) and server are affected by these flaws. These flaws allow a malicious client or server to send specially crafted messages that, when processed by the QUIC image compression algorithm, result in a process crash or potential code execution.	6.6	More Details
CVE-2020-3598	A vulnerability in the web-based management interface of Cisco Vision Dynamic Signage Director could allow an unauthenticated, remote attacker to access confidential information or make configuration changes. The vulnerability is due to missing authentication for a specific section of the web-based management interface. An attacker could exploit this vulnerability by accessing a crafted URL. A successful exploit could allow the attacker to obtain access to a section of the interface, which they could use to read confidential information or make configuration changes.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9122	Some Huawei products have an insufficient input verification vulnerability. Attackers can exploit this vulnerability in the LAN to cause service abnormal on affected devices.Affected product versions include:HiRouter-CD30-10 version 10.0.2.5;HiRouter-CT31-10 version 10.0.2.20;WS5200-12 version 10.0.1.9;WS5281-10 version 10.0.5.10;WS5800-10 version 10.0.3.25;WS7100-10 version 10.0.5.21;WS7200-10 version 10.0.5.21.	6.5	More Details
CVE-2020-5134	A vulnerability in SonicOS allows an authenticated attacker to cause out-of-bound invalid file reference leads to a firewall crash. This vulnerability affected SonicOS Gen 6 version 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version 7.0.0.0.	6.5	More Details
CVE-2020-9230	WS5800-10 version 10.0.3.25 has a denial of service vulnerability. Due to improper verification of specific message, an attacker may exploit this vulnerability to cause specific function to become abnormal.	6.5	More Details
CVE-2020-5136	A buffer overflow vulnerability in SonicOS allows an authenticated attacker to cause Denial of Service (DoS) in the SSL-VPN and virtual assist portal, which leads to a firewall crash. This vulnerability affected SonicOS Gen 5 version 5.9.1.7, 5.9.1.13, Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version 7.0.0.0.	6.5	More Details
CVE-2020-4781	An improper input validation before calling java readLine() method may impact IBM Curam Social Program Management 7.0.9 and 7.0.10, which could result in a denial of service. IBM X-Force ID: 189159.	6.5	More Details
CVE-2020-3567	A vulnerability in the management REST API of Cisco Industrial Network Director (IND) could allow an authenticated, remote attacker to cause the CPU utilization to increase to 100 percent, resulting in a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of requests sent to the REST API. An attacker could exploit this vulnerability by sending a crafted request to the REST API. A successful exploit could allow the attacker to cause a permanent DoS condition that is due to high CPU utilization. Manual intervention may be required to recover the Cisco IND.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3543	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-2020-9238	Taurus-AN00B versions earlier than 10.1.0.156(C00E155R7P2) have a buffer overflow vulnerability. A function in a module does not verify inputs sufficiently. Attackers can exploit this vulnerability by sending specific request. This could compromise normal service of the affected device.	6.5	More Details
CVE-2020-4773	A cross-site request forgery (CSRF) vulnerability may impact IBM Curam Social Program Management 7.0.9 and 7.0.10, which is an attack that forces a user to execute unwanted actions on the web application while they are currently authenticated. This applies to a single server class only, with no impact to remainder of web application. IBM X-Force ID: 189151.	6.5	More Details
CVE-2020-5141	A vulnerability in SonicOS allows a remote unauthenticated attacker to brute force Virtual Assist ticket ID in the firewall SSLVPN service. This vulnerability affected SonicOS Gen 5 version 5.9.1.7, 5.9.1.13, Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version SonicOS 7.0.0.0.	6.5	More Details
CVE-2020-2295	A cross-site request forgery (CSRF) vulnerability in Jenkins Maven Cascade Release Plugin 1.3.2 and earlier allows attackers to start cascade builds and layout builds, and reconfigure the plugin.	6.5	More Details
CVE-2020-15501	Smarter Coffee Maker before 2nd generation allows firmware replacement without authentication or authorization. User interaction is required to press a button. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.5	More Details
CVE-2020-2294	Jenkins Maven Cascade Release Plugin 1.3.2 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission to start cascade builds and layout builds, and reconfigure the plugin.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2293	Jenkins Persona Plugin 2.4 and earlier allows users with Overall/Read permission to read arbitrary files on the Jenkins controller.	6.5	More Details
CVE-2020-13346	Membership changes are not reflected in ToDo subscriptions in GitLab versions prior to 13.2.10, 13.3.7 and 13.4.2, allowing guest users to access confidential issues through API.	6.5	More Details
CVE-2020-5389	Dell EMC OpenManage Integration for Microsoft System Center (OMIMSSC) for SCCM and SCVMM versions prior to 7.2.1 contain an information disclosure vulnerability. Authenticated low privileged OMIMSCC users may be able to retrieve sensitive information from the logs.	6.5	More Details
CVE-2020-2298	Jenkins Nerrvana Plugin 1.02.06 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	6.5	More Details
CVE-2020-17409	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of NETGEAR R6120, R6080, R6260, R6220, R6020, JNR3210, and WNR2020 routers with firmware 1.0.66. Authentication is not required to exploit this vulnerability. The specific flaw exists within the mini_httpd service, which listens on TCP port 80 by default. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-10754.	6.5	More Details
CVE-2020-26922	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WC7500 before 6.5.5.24, WC7600 before 6.5.5.24, WC7600v2 before 6.5.5.24, and WC9500 before 6.5.5.24.	6.4	More Details
CVE-2020-3602	A vulnerability in the CLI of Cisco StarOS operating system for Cisco ASR 5000 Series Routers could allow an authenticated, local attacker to elevate privileges on an affected device. The vulnerability is due to insufficient input validation of CLI commands. An attacker could exploit this vulnerability by sending crafted commands to the CLI. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the root user on the affected device. To exploit this vulnerability, an attacker would need to have valid credentials on an affected device and know the password for the cli test-commands command.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7811	Samsung Update 3.0.2.0 ~ 3.0.32.0 has a vulnerability that allows privilege escalation as commands crafted by attacker are executed while the engine deserializes the data received during inter-process communication	6.2	More Details
CVE-2020-5142	A stored cross-site scripting (XSS) vulnerability exists in the SonicOS SSLVPN web interface. A remote unauthenticated attacker is able to store and potentially execute arbitrary JavaScript code in the firewall SSLVPN portal. This vulnerability affected SonicOS Gen 5 version 5.9.1.7, 5.9.1.13, Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version SonicOS 7.0.0.0.	6.1	More Details
CVE-2020-26870	Cure53 DOMPurify before 2.0.17 allows mutation XSS. This occurs because a serialize-parse roundtrip does not necessarily return the original DOM tree, and a namespace can change from HTML to MathML, as demonstrated by nesting of FORM elements.	6.1	More Details
CVE-2020-26162	Xerox WorkCentre EC7836 before 073.050.059.25300 and EC7856 before 073.020.059.25300 devices allow XSS via Description pages.	6.1	More Details
CVE-2020-25272	In SourceCodester Online Bus Booking System 1.0, there is XSS through the name parameter in book_now.php.	6.1	More Details
CVE-2020-12670	XSS exists in Webmin 1.941 and earlier affecting the Save function of the Read User Email Module / mailboxes Endpoint when attempting to save HTML emails. This module parses any output without sanitizing SCRIPT elements, as opposed to the View function, which sanitizes the input correctly. A malicious user can send any JavaScript payload into the message body and execute it if the user decides to save that email.	6.1	More Details
CVE-2020-24301	Users of the HAPI FHIR Testpage Overlay 5.0.0 and below can use a specially crafted URL to exploit an XSS vulnerability in this module, allowing arbitrary JavaScript to be executed in the user's browser. The impact of this vulnerability is believed to be low, as this module is intended for testing and not believed to be widely used for any production purposes.	6.1	More Details
CVE-2020-26934	phpMyAdmin before 4.9.6 and 5.x before 5.0.3 allows XSS through the transformation feature via a crafted link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26915	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.0	More Details
CVE-2020-13334	In GitLab versions prior to 13.2.10, 13.3.7 and 13.4.2, improper authorization checks allow a non-member of a project/group to change the confidentiality attribute of issue via mutation GraphQL query	5.9	More Details
CVE-2020-3596	A vulnerability in the Session Initiation Protocol (SIP) of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incorrect handling of incoming SIP traffic. An attacker could exploit this vulnerability by sending a series of SIP packets to an affected device. A successful exploit could allow the attacker to exhaust memory on an affected device, causing it to crash and leading to a DoS condition.	5.9	More Details
CVE-2020-13955	HttpUtils#getURLConnection method disables explicitly hostname verification for HTTPS connections making clients vulnerable to man-in-the-middle attacks. Calcite uses internally this method to connect with Druid and Splunk so information leakage may happen when using the respective Calcite adapters. The method itself is in a utility class so people may use it to create vulnerable HTTPS connections for other applications. From Apache Calcite 1.26 onwards, the hostname verification will be performed using the default JVM truststore.	5.9	More Details
CVE-2020-15646	If an attacker intercepts Thunderbird's initial attempt to perform automatic account setup using the Microsoft Exchange autodiscovery mechanism, and the attacker sends a crafted response, then Thunderbird sends username and password over https to a server controlled by the attacker. This vulnerability affects Thunderbird < 68.10.0.	5.9	More Details
CVE-2020-26931	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects WC7500 before 6.5.5.24, WC7600 before 6.5.5.24, WC7600v2 before 6.5.5.24, and WC9500 before 6.5.5.24.	5.9	More Details
CVE-2020-24722	An issue was discovered in the GAEN (aka Google/Apple Exposure Notifications) protocol through 2020-10-05, as used in COVID-19 applications on Android and iOS. The encrypted metadata block with a TX value lacks a checksum, allowing bitflipping to amplify a contamination attack. This can cause metadata deanonymization and risk-score inflation. NOTE: the vendor's position is "We do not believe that TX power authentication would be a useful defense against relay attacks.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3568	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. The vulnerability is due to insufficient input validation of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for the affected device, which could allow malicious URLs to pass through the device.	5.8	More Details
CVE-2020-13344	An issue has been discovered in GitLab affecting all versions prior to 13.2.10, 13.3.7 and 13.4.2. Sessions keys are stored in plain-text in Redis which allows attacker with Redis access to authenticate as any user that has a session stored in Redis	5.7	More Details
CVE-2020-9087	Taurus-AL00A version 10.0.0.1(C00E1R1P1) has an out-of-bounds read vulnerability in XFRM module. An authenticated, local attacker may perform a specific operation to exploit this vulnerability. Due to insufficient validation of the parameters, which may be exploited to cause information leak.	5.5	More Details
CVE-2020-9091	Taurus-AN00B versions earlier than 10.1.0.156(C00E155R7P2) have an out-of-bounds read and write vulnerability. Some functions do not verify inputs sufficiently. Attackers can exploit this vulnerability by sending specific request. This could compromise normal service of the affected device.	5.5	More Details
CVE-2020-9107	HUAWEI P30 Pro versions earlier than 10.1.0.160(C00E160R2P8) have an out-of-bounds read and write vulnerability. An unauthenticated attacker crafts malformed message with specific parameter and sends the message to the affected products. Due to insufficient validation of message, which may be exploited to cause the process reboot.	5.5	More Details
CVE-2020-9108	HUAWEI P30 Pro versions earlier than 10.1.0.160(C00E160R2P8) have an out-of-bounds read and write vulnerability. An unauthenticated attacker crafts malformed message with specific parameter and sends the message to the affected products. Due to insufficient validation of message, which may be exploited to cause the process reboot.	5.5	More Details
CVE-2020-12911	A denial of service vulnerability exists in the D3DKMTCreateAllocation handler functionality of AMD ATIKMDAG.SYS (e.g. version 26.20.15029.27017). A specially crafted D3DKMTCreateAllocation API request can cause an out-of-bounds read and denial of service (BSOD). This vulnerability can be triggered from a non-privileged account.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26164	In kdeconnect-kde (aka KDE Connect) before 20.08.2, an attacker on the local network could send crafted packets that trigger use of large amounts of CPU, memory, or network connection slots, aka a Denial of Service attack.	5.5	More Details
CVE-2020-9240	Taurus-AN00B versions earlier than 10.1.0.156(C00E155R7P2) have a buffer overflow vulnerability. A function in a module does not verify inputs sufficiently. Attackers can exploit this vulnerability by sending specific request. This could compromise normal service of the affected device.	5.5	More Details
CVE-2020-12933	A denial of service vulnerability exists in the D3DKMTEscape handler functionality of AMD ATIKMDAG.SYS (e.g. version 26.20.15029.27017). A specially crafted D3DKMTEscape API request can cause an out-of-bounds read in Windows OS kernel memory area. This vulnerability can be triggered from a non-privileged account.	5.5	More Details
CVE-2020-26567	An issue was discovered on D-Link DSR-250N before 3.17B devices. The CGI script upgradeStatusReboot.cgi can be accessed without authentication. Any access reboots the device, rendering it therefore unusable for several minutes.	5.5	More Details
CVE-2020-13339	An issue has been discovered in GitLab affecting all versions before 13.2.10, 13.3.7 and 13.4.2: XSS in SVG File Preview. Overall impact is limited due to the current user only being impacted.	5.5	More Details
CVE-2020-3597	A vulnerability in the configuration restore feature of Cisco Nexus Data Broker software could allow an unauthenticated, remote attacker to perform a directory traversal attack on an affected device. The vulnerability is due to insufficient validation of configuration backup files. An attacker could exploit this vulnerability by persuading an administrator to restore a crafted configuration backup file. A successful exploit could allow the attacker to overwrite arbitrary files that are accessible through the affected software on an affected device.	5.4	More Details
CVE-2020-14184	Affected versions of Atlassian Jira Server allow remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in Jira issue filter export files. The affected versions are before 8.5.9, from version 8.6.0 before 8.12.3, and from version 8.13.0 before 8.13.1.	5.4	More Details
CVE-2020-4681	IBM Security Guardium 11.2 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: 186427.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4680	IBM Security Guardium 11.2 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: 186426.	5.4	More Details
CVE-2020-26916	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JR6150 before 1.0.1.24, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.64, R6700v2 before 1.2.0.62, R6800 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.50, and WNR2020 before 1.1.0.62.	5.4	More Details
CVE-2020-25270	PHPGurukul hostel-management-system 2.1 allows XSS via Guardian Name, Guardian Relation, Guardian Contact no, Address, or City.	5.4	More Details
CVE-2020-8820	An XSS Vulnerability exists in Webmin 1.941 and earlier affecting the Cluster Shell Commands Endpoint. A user may enter any XSS Payload into the Command field and execute it. Then, after revisiting the Cluster Shell Commands Menu, the XSS Payload will be rendered and executed.	5.4	More Details
CVE-2020-8821	An Improper Data Validation Vulnerability exists in Webmin 1.941 and earlier affecting the Command Shell Endpoint. A user may enter HTML code into the Command field and submit it. Then, after visiting the Action Logs Menu and displaying logs, the HTML code will be rendered (however, JavaScript is not executed). Changes are kept across users.	5.4	More Details
CVE-2020-25271	PHPGurukul hospital-management-system-in-php 4.0 allows XSS via admin/patient-search.php, doctor/search.php, book-appointment.php, doctor/appointment-history.php, or admin/appointment-history.php.	5.4	More Details
CVE-2020-3536	A vulnerability in the web-based management interface of Cisco SD-WAN vManage 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 inserting malicious data into a specific data field in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface.	5.4	More Details
CVE-2020-2289	Jenkins Active Choices Plugin 2.4 and earlier does not escape the name and description of build parameters, 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-2020-2290	Jenkins Active Choices Plugin 2.4 and earlier does not escape some return values of sandboxed scripts for Reactive Reference Parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2020-2292	Jenkins Release Plugin 2.10.2 and earlier does not escape the release version in badge tooltip, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Release/Release permission.	5.4	More Details
CVE-2020-3320	A vulnerability in the web-based management interface of Cisco Firepower Management Center could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by first entering input within the web-based management interface and then persuading a user of the interface to view the crafted input within 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.	5.4	More Details
CVE-2020-4775	A cross-site scripting (XSS) vulnerability may impact IBM Curam Social Program Management 7.0.9 and 7.0.10. This vulnerability allows attackers to inject malicious scripts into web applications for the purpose of running unwanted actions on the end user's device, restricted to a single location. IBM X-Force ID: 189153.	5.4	More Details
CVE-2020-4774	An XPath vulnerability may impact IBM Curam Social Program Management 7.0.9 and 7.0.10, caused by the improper handling of user-supplied input. By sending a specially-crafted input, a remote attacker could exploit this vulnerability to obtain unauthorized access or reveal sensitive information such as XML document structure and content. IBM X-Force ID: 189152.	5.4	More Details
CVE-2020-25343	Cross-site scripting (XSS) vulnerabilities in Symphony CMS 3.0.0 allow remote attackers to inject arbitrary web script or HTML to fields['body'] param via events\event.publish_article.php	5.4	More Details
CVE-2020-4741	IBM InfoSphere Information Server 11.5 and 11.7 is vulnerable to stored 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: 188197.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2287	Jenkins Audit Trail Plugin 3.6 and earlier applies pattern matching to a different representation of request URL paths than the Stapler web framework uses for dispatching requests, which allows attackers to craft URLs that bypass request logging of any target URL.	5.3	More Details
CVE-2020-2288	In Jenkins Audit Trail Plugin 3.6 and earlier, the default regular expression pattern could be bypassed in many cases by adding a suffix to the URL that would be ignored during request handling.	5.3	More Details
CVE-2020-15217	In GLPI before version 9.5.2, there is a leakage of user information through the public FAQ. The issue was introduced in version 9.5.0 and patched in 9.5.2. As a workaround, disable public access to the FAQ.	5.3	More Details
CVE-2020-4699	IBM Security Access Manager 9.0.7 and IBM Security Verify Access 10.0.0 could allow an attacker to obtain sensitive using timing side channel attacks which could aid in further attacks against the system. IBM X-Force ID: 186947.	5.3	More Details
CVE-2020-4661	IBM Security Access Manager 9.0.7 and IBM Security Verify Access 10.0.0 could allow an attacker to obtain sensitive using timing side channel attacks which could aid in further attacks against the system. IBM X-Force ID: 186142.	5.3	More Details
CVE-2020-4660	IBM Security Access Manager 9.0.7 and IBM Security Verify Access 10.0.0 could allow an attacker to obtain sensitive using timing side channel attacks which could aid in further attacks against the system. IBM X-Force ID: 186140.	5.3	More Details
CVE-2020-4780	OOTB build scripts does not set the secure attribute on session cookie which may impact IBM Curam Social Program Management 7.0.9 and 7.0,10. The purpose of the 'secure' attribute is to prevent cookies from being observed by unauthorized parties. IBM X-Force ID: 189158.	5.3	More Details
CVE-2020-25867	SoPlanning before 1.47 doesn't correctly check the security key used to publicly share plannings. It allows a bypass to get access without authentication.	5.3	More Details
CVE-2020-5143	SonicOS SSLVPN login page allows a remote unauthenticated attacker to perform firewall management administrator username enumeration based on the server responses. This vulnerability affected SonicOS Gen 5 version 5.9.1.7, 5.9.1.13, Gen 6 version 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v and Gen 7 version SonicOS 7.0.0.0.	5.3	More Details
CVE-2020-25768	Contao before 4.4.52, 4.9.x before 4.9.6, and 4.10.x before 4.10.1 have Improper Input Validation. It is possible to inject insert tags in front end forms which will be replaced when the page is rendered.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4740	IBM InfoSphere Information Server 11.5 and 11.7 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 188150.	5.2	More Details
CVE-2020-15226	In GLPI before version 9.5.2, there is a SQL Injection in the API's search function. Not only is it possible to break the SQL syntax, but it is also possible to utilise a UNION SELECT query to reflect sensitive information such as the current database version, or database user. The most likely scenario for this vulnerability is with someone who has an API account to the system. The issue is patched in version 9.5.2. A proof-of-concept with technical details is available in the linked advisory.	5.0	More Details
CVE-2020-4678	IBM Security Guardium 11.2 could allow an attacker with admin access to obtain and read files that they normally would not have access to. IBM X-Force ID: 186423.	4.9	More Details
CVE-2020-13341	An issue has been discovered in GitLab affecting all versions prior to 13.2.10, 13.3.7 and 13.4.2. Insufficient permission check allows attacker with developer role to perform various deletions.	4.9	More Details
CVE-2020-17551	ImpressCMS 1.4.0 is affected by XSS in modules/system/admin.php which may result in arbitrary remote code execution.	4.8	More Details
CVE-2020-3589	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker with administrative credentials 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 injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker would need to have valid administrative credentials.	4.8	More Details
CVE-2020-4679	IBM Security Guardium 11.2 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: 186424.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15241	TYPO3 Fluid Engine (package `typo3fluid/fluid`) before versions 2.0.5, 2.1.4, 2.2.1, 2.3.5, 2.4.1, 2.5.5 or 2.6.1 is vulnerable to cross-site scripting when making use of the ternary conditional operator in templates like `{showFullName ? fullName : defaultValue}`. Updated versions of this package are bundled in following TYPO3 (`typo3/cms-core`) versions as well: TYPO3 v8.7.25 (using `typo3fluid/fluid` v2.5.4) and TYPO3 v9.5.6 (using `typo3fluid/fluid` v2.6.1).	4.7	More Details
CVE-2020-12401	During ECDSA signature generation, padding applied in the nonce designed to ensure constant-time scalar multiplication was removed, resulting in variable-time execution dependent on secret data. This vulnerability affects Firefox < 80 and Firefox for Android < 80.	4.7	More Details
CVE-2020-15242	Next.js versions >=9.5.0 and <9.5.4 are vulnerable to an Open Redirect. Specially encoded paths could be used with the trailing slash redirect to allow an open redirect to occur to an external site. In general, this redirect does not directly harm users although can allow for phishing attacks by redirecting to an attackers domain from a trusted domain. The issue is fixed in version 9.5.4.	4.7	More Details
CVE-2020-12400	When converting coordinates from projective to affine, the modular inversion was not performed in constant time, resulting in a possible timing-based side channel attack. This vulnerability affects Firefox < 80 and Firefox for Android < 80.	4.7	More Details
CVE-2020-9110	Taurus-AN00B versions earlier than 10.1.0.156(C00E155R7P2) have an information disclosure vulnerability. The device does not sufficiently validate the output of device in certain specific scenario, the attacker can gain information in the victim's smartphone to launch the attack, successful exploit could cause information disclosure.	4.6	More Details
CVE-2020-9109	There is an information disclosure vulnerability in several smartphones. The device does not sufficiently validate the identity of smart wearable device in certain specific scenario, the attacker need to gain certain information in the victim's smartphone to launch the attack, and successful exploit could cause information disclosure.Affected product versions include:HUAWEI Mate 20 versions earlier than 10.1.0.160(C00E160R3P8),versions earlier than 10.1.0.160(C01E160R2P8);HUAWEI Mate 20 X versions earlier than 10.1.0.160(C00E160R2P8),versions earlier than 10.1.0.160(C01E160R2P8);HUAWEI P30 Pro versions earlier than 10.1.0.160(C00E160R2P8);Laya-AL00EP versions earlier than 10.1.0.160(C786E160R3P8);Tony-AL00B versions earlier than 10.1.0.160(C00E160R2P11);Tony-TL00B versions earlier than 10.1.0.160(C01E160R2P11).	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9106	HUAWEI P30 Pro versions earlier than 10.1.0.160(C00E160R2P8) have a path traversal vulnerability. The system does not sufficiently validate certain pathname, successful exploit could allow the attacker access files and cause information disclosure.	4.6	More Details
CVE-2020-13626	OnePlus App Locker through 2020-10-06 allows physically proximate attackers to use Google Assistant to bypass an authorization check in order to send an SMS message when the SMS application is locked.	4.6	More Details
CVE-2020-3601	A vulnerability in the CLI of Cisco StarOS operating system for Cisco ASR 5000 Series Routers could allow an authenticated, local attacker to elevate privileges on an affected device. The vulnerability is due to insufficient input validation of CLI commands. An attacker could exploit this vulnerability by sending crafted commands to the CLI. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the root user. To exploit this vulnerability, an attacker would need to have valid administrative credentials on an affected device.	4.4	More Details
CVE-2020-15250	In JUnit4 from version 4.7 and before 4.13.1, the test rule TemporaryFolder contains a local information disclosure vulnerability. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. This vulnerability impacts you if the JUnit tests write sensitive information, like API keys or passwords, into the temporary folder, and the JUnit tests execute in an environment where the OS has other untrusted users. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. For Java 1.7 and higher users: this vulnerability is fixed in 4.13.1. For Java 1.6 and lower users: no patch is available, you must use the workaround below. If you are unable to patch, or are stuck running on Java 1.6, specifying the `java.io.tmpdir` system environment variable to a directory that is exclusively owned by the executing user will fix this vulnerability. For more information, including an example of vulnerable code, see the referenced GitHub Security Advisory.	4.4	More Details
CVE-2020-2296	A cross-site request forgery (CSRF) vulnerability in Jenkins Shared Objects Plugin 0.44 and earlier allows attackers to configure shared objects.	4.3	More Details
CVE-2020-13335	Improper group membership validation when deleting a user account in GitLab >=7.12 allows a user to delete own account without deleting/transferring their group.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26932	debian/sympa.postinst for the Debian Sympa package before 6.2.40~dfsg-7 uses mode 4755 for sympa_newaliases-wrapper, whereas the intended permissions are mode 4750 (for access by the sympa group)	4.3	More Details
CVE-2020-13943	If an HTTP/2 client connecting to Apache Tomcat 10.0.0-M1 to 10.0.0-M7, 9.0.0.M1 to 9.0.37 or 8.5.0 to 8.5.57 exceeded the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it was possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This could lead to users seeing responses for unexpected resources.	4.3	More Details
CVE-2020-26923	Certain NETGEAR devices are affected by stored XSS. This affects WC7500 before 6.5.5.24, WC7600 before 6.5.5.24, WC7600v2 before 6.5.5.24, and WC9500 before 6.5.5.24.	4.3	More Details
CVE-2020-25262	PyroCMS 3.7 is vulnerable to cross-site request forgery (CSRF) via the admin/pages/delete/ URI: pages will be deleted.	4.3	More Details
CVE-2020-26918	Certain NETGEAR devices are affected by stored XSS. This affects EX7000 before 1.0.1.78, R6250 before 1.0.4.34, R6400 before 1.0.1.46, R6400v2 before 1.0.2.66, R6700v3 before 1.0.2.66, R7100LG before 1.0.0.50, R7300DST before 1.0.0.70, R7900 before 1.0.3.8, R8300 before 1.0.2.128, and R8500 before 1.0.2.128.	4.1	More Details
CVE-2020-26917	Certain NETGEAR devices are affected by stored XSS. This affects EX7000 before 1.0.1.78, R6250 before 1.0.4.34, R6400 before 1.0.1.46, R6400v2 before 1.0.2.66, R7100LG before 1.0.0.50, R7300DST before 1.0.0.70, R7900 before 1.0.3.8, R8300 before 1.0.2.128, and R8500 before 1.0.2.128.	4.1	More Details
CVE-2020-26930	NETGEAR EX7700 devices before 1.0.0.210 are affected by incorrect configuration of security settings.	3.3	More Details
CVE-2020-2297	Jenkins SMS Notification Plugin 1.2 and earlier stores an access token unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	3.3	More Details
CVE-2020-25779	Trend Micro Antivirus for Mac 2020 (Consumer) has a vulnerability in which a Internationalized Domain Name homograph attack (Puny-code) could be used to add a malicious website to the approved websites list of Trend Micro Antivirus for Mac to bypass the web threat protection feature.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2291	Jenkins couchdb-statistics Plugin 0.3 and earlier stores its server password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	3.3	More Details
CVE-2020-17411	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 10.0.0.35798. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11190.	3.3	More Details
CVE-2020-26925	NETGEAR GS808E devices before 1.7.1.0 are affected by denial of service.	3.2	More Details
CVE-2020-26924	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects WAC720 before 3.9.1.13 and WAC730 before 3.9.1.13.	3.1	More Details
CVE-2020-13342	An issue has been discovered in GitLab affecting versions prior to 13.2.10, 13.3.7 and 13.4.2: Lack of Rate Limiting at Re-Sending Confirmation Email	2.7	More Details
CVE-2015-7380	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2015-7379	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-13332	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-13903	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-12254. Reason: This candidate is a reservation duplicate of CVE-2020-12254. Notes: All CVE users should reference CVE-2020-12254 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details