SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 18 November 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-2020-27485	Garmin Forerunner 235 before 8.20 is affected by: Array index error. The component is: ConnectIQ TVM. The attack vector is: To exploit the vulnerability, the attacker must upload a malicious ConnectIQ application to the ConnectIQ store. The ConnectIQ program interpreter fails to check the index provided when accessing the local variable in the LGETV and LPUTV instructions. This provides the ability to both read and write memory outside the bounds of the TVM context allocation. It can be leveraged to construct a use-after-free scenario, leading to a constrained read/write primitive across the entire MAX32630 address space. A successful exploit would allow a ConnectIQ app store application to escape and perform activities outside the restricted application execution environment.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27484	Garmin Forerunner 235 before 8.20 is affected by: Integer Overflow. The component is: ConnectIQ TVM. The attack vector is: To exploit the vulnerability, the attacker must upload a malicious ConnectIQ application to the ConnectIQ store. The ConnectIQ program interpreter fails to check for overflow when allocating the array for the NEWA instruction. This a constrained read/write primitive across the entire MAX32630 address space. A successful exploit would allow a ConnectIQ app store application to escape and perform activities outside the restricted application execution environment.	9.9	More Details
CVE-2020-13774	An unrestricted file-upload issue in EditLaunchPadDialog.aspx in Ivanti Endpoint Manager 2019.1 and 2020.1 allows an authenticated attacker to gain remote code execution by uploading a malicious aspx file. The issue is caused by insufficient file extension validation and insecure file operations on the uploaded image, which upon failure will leave the temporarily created files in an accessible location on the server.	9.9	More Details
CVE-2020-27486	Garmin Forerunner 235 before 8.20 is affected by: Buffer Overflow. The component is: ConnectIQ TVM. The attack vector is: To exploit the vulnerability, the attacker must upload a malicious ConnectIQ application to the ConnectIQ store. The ConnectIQ program interpreter trusts the string length provided in the data section of the PRG file. It allocates memory for the string immediately, and then copies the string into the TVM object by using a function similar to strcpy. This copy can exceed the length of the allocated string data and overwrite heap data. A successful exploit would allow a ConnectIQ app store application to escape and perform activities outside the restricted application execution environment.	9.9	More Details
CVE-2020-27483	Garmin Forerunner 235 before 8.20 is affected by: Array index error. The component is: ConnectIQ TVM. The attack vector is: To exploit the vulnerability, the attacker must upload a malicious ConnectIQ application to the ConnectIQ store. The ConnectIQ program interpreter trusts the offset provided for the stack value duplication instruction, DUP. The offset is unchecked and memory prior to the start of the execution stack can be read and treated as a TVM object. A successful exploit could use the vulnerability to leak runtime information such as the heap handle or pointer for a number of TVM context variables. Some reachable values may be controlled enough to forge a TVM object on the stack, leading to possible remote code execution.	9.9	More Details
CVE-2020-5664	Deserialization of untrusted data vulnerability in XooNIps 3.49 and earlier allows remote attackers to execute arbitrary code via unspecified vectors.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25207	JetBrains ToolBox before version 1.18 is vulnerable to Remote Code Execution via a browser protocol handler.	9.8	More Details
CVE-2020-25952	SQL injection vulnerability in PHPGurukul User Registration & Login and User Management System With admin panel 2.1 allows remote attackers to execute arbitrary SQL commands and bypass authentication.	9.8	More Details
CVE-2020-27422	In Anuko Time Tracker v1.19.23.5311, the password reset link emailed to the user doesn't expire once used, allowing an attacker to use the same link to takeover the account.	9.8	More Details
CVE-2020-26508	The WebTools component on Canon Oce ColorWave 3500 5.1.1.0 devices allows attackers to retrieve stored SMB credentials via the export feature, even though these are intentionally inaccessible in the UI.	9.8	More Details
CVE-2020-26510	Airleader Master <= 6.21 devices have default credentials that can be used to access the exposed Tomcat Manager for deployment of a new .war file, with resultant remote code execution.	9.8	More Details
CVE-2020-17051	Windows Network File System Remote Code Execution Vulnerability	9.8	More Details
CVE-2020-5426	Scheduler for TAS prior to version 1.4.0 was permitting plaintext transmission of UAA client token by sending it over a non-TLS connection. This also depended on the configuration of the MySQL server which is used to cache a UAA client token used by the service. If intercepted the token can give an attacker admin level access in the cloud controller.	9.8	More Details
CVE-2020-11851	Arbitrary code execution vulnerability on Micro Focus ArcSight Logger product, affecting all version prior to 7.1.1. The vulnerability could be remotely exploited resulting in the execution of arbitrary code.	9.8	More Details
CVE-2020-27555	Use of default credentials for the telnet server in BASETech GE-131 BT-1837836 firmware 20180921 allows remote attackers to execute arbitrary system commands as the root user.	9.8	More Details
CVE-2020-28138	SourceCodester Online Clothing Store 1.0 is affected by a SQL Injection via the txtUserName parameter to login.php.	9.8	More Details
CVE-2020-28140	SourceCodester Online Clothing Store 1.0 is affected by an arbitrary file upload via the image upload feature of Products.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28133	An issue was discovered in SourceCodester Simple Grocery Store Sales And Inventory System 1.0. There was authentication bypass in web login functionality allows an attacker to gain client privileges via SQL injection in sales_inventory/login.php.	9.8	More Details
CVE-2020-26553	An issue was discovered in Aviatrix Controller before R6.0.2483. Several APIs contain functions that allow arbitrary files to be uploaded to the web tree.	9.8	More Details
CVE-2020-28130	An Arbitrary File Upload in the Upload Image component in SourceCodester Online Library Management System 1.0 allows the user to conduct remote code execution via admin/borrower/index.php?view=add because .php files can be uploaded to admin/borrower/photos (under the web root).	9.8	More Details
CVE-2020-28642	In InfiniteWP Admin Panel before 3.1.12.3, resetPasswordSendMail generates a weak password-reset code, which makes it easier for remote attackers to conduct admin Account Takeover attacks.	9.8	More Details
CVE-2020-8271	Unauthenticated remote code execution with root privileges in Citrix SD-WAN Center versions before 11.2.2, 11.1.2b and 10.2.8	9.8	More Details
CVE-2020-28638	ask_password in Tomb 2.0 through 2.7 returns a warning when pinentry-curses is used and $DISPLAY is non-empty, causing affected users' files to be encrypted with "tomb {W] Detected DISPLAY, but only pinentry-curses is found." as the encryption key.	9.8	More Details
CVE-2020-13638	lib/crud/userprocess.php in rConfig 3.9.x before 3.9.7 has an authentication bypass, leading to administrator account creation. This issue has been fixed in 3.9.7.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11168	u'Null-pointer dereference can occur while accessing data buffer beyond its size that leads to access the buffer beyond its range' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8009W, APQ8017, APQ8053, APQ8064AU, APQ8096AU, APQ8098, MDM9206, MDM9650, MSM8909W, MSM8953, MSM8996AU, QCM4290, QCS405, QCS4290, QCS603, QCS605, QM215, QSM8350, SA6155, SA6155P, SA8155, SA8155P, SDA429W, SDA640, SDA660, SDA845, SDA855, SDM1000, SDM429, SDM429W, SDM450, SDM632, SDM640, SDM830, SDM845, SDW2500, SDX20, SDX20M, SDX50M, SDX55, SDX55M, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6250, SM6350, SM7125, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SM8350, SM8350P, SXR2130, SXR2130P, WCD9330	9.8	More Details
CVE-2020-11184	u'Possible buffer overflow will occur in video while parsing mp4 clip with crafted esds atom size.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile in QCM4290, QCS4290, QM215, QSM8350, SA6145P, SA6155, SA6155P, SA8155, SA8155P, SDX55, SDX55M, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6250, SM6350, SM7125, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SM8350, SM8350P, SXR2130, SXR2130P	9.8	More Details
CVE-2020-11193	u'Buffer over read can happen while parsing mkv clip due to improper typecasting of data returned from atomsize' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8009W, APQ8017, APQ8037, APQ8053, APQ8064AU, APQ8096, APQ8096AU, APQ8096SG, APQ8098, MDM9206, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8996SG, MSM8998, QCM4290, QCM6125, QCS405, QCS410, QCS4290, QCS603, QCS605, QCS610, QCS6125, QM215, QSM8350, SA6145P, SA6155, SA6155P, SA8155, SA8155P, SDA429W, SDA640, SDA660, SDA670, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM455, SDM630, SDM632, SDM636, SDM640, SDM660, SDM670, SDM710, SDM830, SDM845, SDW2500, SDX20, SDX20M, SDX50M, SDX55, SDX55M, SM4125, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6150, SM6150P, SM6250, SM6250P, SM6350, SM7125, SM7150, SM7150P, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SM8350, SM8350P, SXR1120, SXR1130, SXR2130, SXR2130P, WCD9330	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11196	u'Integer overflow to buffer overflow occurs while playback of ASF clip having unexpected number of codec entries' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8009W, APQ8017, APQ8037, APQ8053, APQ8064AU, APQ8096, APQ8096AU, APQ8096SG, APQ8098, MDM9206, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8996SG, MSM8998, QCM4290, QCM6125, QCS405, QCS410, QCS4290, QCS603, QCS605, QCS610, QCS6125, QM215, SA6145P, SA6150P, SA6155, SA6155P, SA8150P, SA8155, SA8155P, SA8195P, SDA429W, SDA640, SDA660, SDA670, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM455, SDM630, SDM632, SDM636, SDM640, SDM660, SDM670, SDM710, SDM830, SDM845, SDW2500, SDX20, SDX20M, SDX50M, SDX55, SDX55M, SM4125, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6150, SM6150P, SM6250, SM6250P, SM6350, SM7125, SM7150, SM7150P, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SXR1120, SXR1130, SXR2130, SXR2130P, WCD9330	9.8	More Details
CVE-2020-3639	u'When a non standard SIP sigcomp message is received from the network, then there may be chances of using more UDVM cycle or memory overflow' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8037, APQ8053, MDM9250, MDM9607, MDM9628, MDM9640, MDM9650, MSM8108, MSM8208, MSM8209, MSM8608, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCM4290, QCM6125, QCS410, QCS4290, QCS603, QCS605, QCS610, QCS6125, QM215, QSM8350, SA415M, SA6145P, SA6150P, SA6155P, SA8150P, SA8155, SA8155P, SA8195P, SC7180, SC8180X, SC8180X+SDX55, SC8180XP, SDA429W, SDA640, SDA660, SDA670, SDA845, SDA855, SDM1000, SDM429, SDM429W, SDM439, SDM450, SDM455, SDM630, SDM632, SDM636, SDM640, SDM660, SDM670, SDM710, SDM712, SDM845, SDM850, SDX24, SDX50M, SDX55, SDX55M, SM4125, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6150, SM6150P, SM6250, SM6250P, SM7125, SM7150, SM7150P, SM7250, SM7250P, SM8150, SM8150P, SM8350, SM8350P, SXR1120, SXR1130	9.8	More Details
CVE-2020-27481	An unauthenticated SQL Injection vulnerability in Good Layers LMS Plugin <= 2.1.4 exists due to the usage of "wp_ajax_nopriv" call in WordPress, which allows any unauthenticated user to get access to the function "gdlr_lms_cancel_booking" where POST Parameter "id" was sent straight into SQL query without sanitization.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28269	Prototype pollution vulnerability in 'field' versions 0.0.1 through 1.0.1 allows attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2020-28270	Prototype pollution vulnerability in 'object-hierarchy-access' versions 0.2.0 through 0.32.0 allows attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2020-28271	Prototype pollution vulnerability in 'deephas' versions 1.0.0 through 1.0.5 allows attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2020-7472	An authorization bypass and PHP local-file-include vulnerability in the installation component of SugarCRM before 8.0, 8.0 before 8.0.7, 9.0 before 9.0.4, and 10.0 before 10.0.0 allows for unauthenticated remote code execution against a configured SugarCRM instance via crafted HTTP requests. (This is exploitable even after installation is completed.).	9.8	More Details
CVE-2020-8752	Out-of-bounds write in IPv6 subsystem for Intel(R) AMT, Intel(R) ISM versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 14.0.45 may allow an unauthenticated user to potentially enable escalation of privileges via network access.	9.8	More Details
CVE-2020-12315	Path traversal in the Intel(R) EMA before version 1.3.3 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	9.8	More Details
CVE-2020-13877	SQL Injection issues in various ASPX pages of ResourceXpress Meeting Monitor 4.9 could lead to remote code execution and information disclosure.	9.8	More Details
CVE-2020-24719	Exposed Erlang Cookie could lead to Remote Command Execution (RCE) attack. Communication between Erlang nodes is done by exchanging a shared secret (aka "magic cookie"). There are cases where the magic cookie is included in the content of the logs. An attacker can use the cookie to attach to an Erlang node and run OS level commands on the system running the Erlang node. Affects version: 6.5.1. Fix version: 6.6.0.	9.8	More Details
CVE-2020-12338	Insufficient control flow management in the Open WebRTC Toolkit before version 4.3.1 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	9.8	More Details
CVE-2020-28183	SQL injection vulnerability in SourceCodester Water Billing System 1.0 via the username and password parameters to process.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27130	A vulnerability in Cisco Security Manager could allow an unauthenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper validation of directory traversal character sequences within requests to an affected device. An attacker could exploit this vulnerability by sending a crafted request to the affected device. A successful exploit could allow the attacker to download arbitrary files from the affected device.	9.1	More Details
CVE-2020-8747	Out-of-bounds read in subsystem for Intel(R) AMT versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70 and 14.0.45 may allow an unauthenticated user to potentially enable information disclosure and/or denial of service via network access.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-23489	The import.json.php file before 8.9 for Avideo is vulnerable to a File Deletion vulnerability. This allows the deletion of configuration.php, which leads to certain privilege checks not being in place, and therefore a user can escalate privileges to admin.	8.8	More Details
CVE-2020-25557	In CMSuno 1.6.2, an attacker can inject malicious PHP code as a "username" while changing his/her username & password. After that, when attacker logs in to the application, attacker's code will be run. As a result of this vulnerability, authenticated user can run command on the server.	8.8	More Details
CVE-2020-28687	The edit profile functionality in ARTWORKS GALLERY IN PHP, CSS, JAVASCRIPT, AND MYSQL 1.0 allows remote attackers to upload arbitrary files.	8.8	More Details
CVE-2020-12321	Improper buffer restriction in some Intel(R) Wireless Bluetooth(R) products before version 21.110 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-13769	LDMS/alert_log.aspx in Ivanti Endpoint Manager through 2020.1 allows SQL Injection via a /remotecontrolauth/api/device request.	8.8	More Details
CVE-2020-17042	Windows Print Spooler Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12313	Insufficient control flow management in some Intel(R) PROSet/Wireless WiFi products before version 21.110 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-12347	Improper input validation in the Intel(R) Data Center Manager Console before version 3.6.2 may allow an authenticated user to potentially enable escalation of privilege via network access.	8.8	More Details
CVE-2020-5659	SQL injection vulnerability in the XooNIps 3.49 and earlier allows remote authenticated attackers to execute arbitrary SQL commands via unspecified vectors.	8.8	More Details
CVE-2020-8749	Out-of-bounds read in subsystem for Intel(R) AMT versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70 and 14.0.45 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-25695	A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. An attacker having permission to create non-temporary objects in at least one schema can execute arbitrary SQL functions under the identity of a superuser. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.8	More Details
CVE-2020-28649	The orbisius-child-theme-creator plugin before 1.5.2 for WordPress allows CSRF via orbisius_ctc_theme_editor_manage_file.	8.8	More Details
CVE-2020-28648	Improper input validation in the Auto-Discovery component of Nagios XI before 5.7.5 allows an authenticated attacker to execute remote code.	8.8	More Details
CVE-2020-8273	Privilege escalation of an authenticated user to root in Citrix SD-WAN center versions before 11.2.2, 11.1.2b and 10.2.8.	8.8	More Details
CVE-2020-28688	The add artwork functionality in ARTWORKS GALLERY IN PHP, CSS, JAVASCRIPT, AND MYSQL 1.0 allows remote attackers to upload arbitrary files.	8.8	More Details
CVE-2020-8270	An unprivileged Windows user on the VDA or an SMB user can perform arbitrary command execution as SYSTEM in CVAD versions before 2009, 1912 LTSR CU1 hotfixes CTX285871 and CTX285872, 7.15 LTSR CU6 hotfix CTX285341 and CTX285342	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27386	An unrestricted file upload issue in FlexDotnetCMS before v1.5.9 allows an authenticated remote attacker to upload and execute arbitrary files by using the FileManager to upload malicious code (e.g., ASP code) in the form of a safe file type (e.g., a TXT file), and then using the FileEditor (in v1.5.8 and prior) or the FileManager's rename function (in v1.5.7 and prior) to rename the file to an executable extension (e.g., ASP), and finally executing the file via an HTTP GET request to /<path_to_file>.	8.8	More Details
CVE-2020-26548	An issue was discovered in Aviatrix Controller before R5.4.1290. There is an insecure sudo rule: a user exists that can execute all commands as any user on the system.	8.8	More Details
CVE-2020-4700	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.2 and 5.2.0.0 through 5.2.6.5 could allow an authenticated user belonging to a specific user group to create a user or group with administrative privileges. IBM X-Force ID: 187077.	8.8	More Details
CVE-2020-25538	An authenticated attacker can inject malicious code into "lang" parameter in /uno/central.php file in CMSuno 1.6.2 and run this PHP code in the web page. In this way, attacker can takeover the control of the server.	8.8	More Details
CVE-2020-4655	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.2 and 5.2.0.0 through 5.2.6.5 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 186091.	8.8	More Details
CVE-2020-17061	Microsoft SharePoint Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-8269	An unprivileged Windows user on the VDA can perform arbitrary command execution as SYSTEM in CVAD versions before 2009, 1912 LTSR CU1 hotfixes CTX285870 and CTX286120, 7.15 LTSR CU6 hotfix CTX285344 and 7.6 LTSR CU9	8.8	More Details
CVE-2020-7841	Improper input validation vulnerability exists in TOBESOFT XPLATFORM which could cause arbitrary .hta file execution when the command string is begun with http://, https://, mailto://	8.8	More Details
CVE-2020-28693	An unrestricted file upload issue in HorizontCMS 1.0.0-beta allows an authenticated remote attacker to upload PHP code through a zip file by uploading a theme, and executing the PHP file via an HTTP GET request to /themes/<php_file_name>	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4647	IBM Sterling File Gateway 2.2.0.0 through 2.2.6.5 and 6.0.0.0 through 6.0.3.2 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database.	8.8	More Details
CVE-2020-26804	In Sentrifugo 3.2, users can share an announcement under "Organization -> Announcements" tab. Also, in this page, users can upload attachments with the shared announcements. This "Upload Attachment" functionality is suffered from "Unrestricted File Upload" vulnerability so attacker can upload malicious files using this functionality and control the server.	8.8	More Details
CVE-2020-28136	An Arbitrary File Upload is discovered in SourceCodester Tourism Management System 1.0 allows the user to conduct remote code execution via admin/create-package.php vulnerable page.	8.8	More Details
CVE-2020-26803	In Sentrifugo 3.2, users can upload an image under "Assets -> Add" tab. This "Upload Images" functionality is suffered from "Unrestricted File Upload" vulnerability so attacker can upload malicious files using this functionality and control the server.	8.8	More Details
CVE-2020-26225	In PrestaShop Product Comments before version 4.2.0, an attacker could inject malicious web code into the users' web browsers by creating a malicious link. The problem was introduced in version 4.0.0 and is fixed in 4.2.0	8.7	More Details
CVE-2020-15275	MoinMoin is a wiki engine. In MoinMoin before version 1.9.11, an attacker with write permissions can upload an SVG file that contains malicious javascript. This javascript will be executed in a user's browser when the user is viewing that SVG file on the wiki. Users are strongly advised to upgrade to a patched version. MoinMoin Wiki 1.9.11 has the necessary fixes and also contains other important fixes.	8.7	More Details
CVE-2020-26222	Dependabot is a set of packages for automated dependency management for Ruby, JavaScript, Python, PHP, Elixir, Rust, Java, .NET, Elm and Go. In Dependabot-Core from version 0.119.0.beta1 before version 0.125.1, there is a remote code execution vulnerability in dependabot-common and dependabot-go_modules when a source branch name contains malicious injectable bash code. For example, if Dependabot is configured to use the following source branch name: "/$({curl,127.0.0.1})", Dependabot will make a HTTP request to the following URL: 127.0.0.1 when cloning the source repository. The fix was applied to version 0.125.1. As a workaround, one can escape the branch name prior to passing it to the Dependabot::Source class.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26070	A vulnerability in the ingress packet processing function of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource allocation when an affected device processes network traffic in software switching mode (punted). An attacker could exploit this vulnerability by sending specific streams of Layer 2 or Layer 3 protocol data units (PDUs) to an affected device. A successful exploit could cause the affected device to run out of buffer resources, which could make the device unable to process or forward traffic, resulting in a DoS condition. The device would need to be restarted to regain functionality.	8.6	More Details
CVE-2020-7769	This affects the package nodemailer before 6.4.16. Use of crafted recipient email addresses may result in arbitrary command flag injection in sendmail transport for sending mails.	8.6	More Details
CVE-2020-17084	Microsoft Exchange Server Remote Code Execution Vulnerability	8.5	More Details
CVE-2020-2050	An authentication bypass vulnerability exists in the GlobalProtect SSL VPN component of Palo Alto Networks PAN-OS software that allows an attacker to bypass all client certificate checks with an invalid certificate. A remote attacker can successfully authenticate as any user and gain access to restricted VPN network resources when the gateway or portal is configured to rely entirely on certificate-based authentication. Impacted features that use SSL VPN with client certificate verification are: GlobalProtect Gateway, GlobalProtect Portal, GlobalProtect Clientless VPN In configurations where client certificate verification is used in conjunction with other authentication methods, the protections added by the certificate check are ignored as a result of this issue. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.17; PAN-OS 9.0 versions earlier than PAN-OS 9.0.11; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5; PAN-OS 10.0 versions earlier than PAN-OS 10.0.1.	8.2	More Details
CVE-2020-27131	Multiple vulnerabilities in the Java deserialization function that is used by Cisco Security Manager could allow an unauthenticated, remote attacker to execute arbitrary commands on an affected device. These vulnerabilities are due to insecure deserialization of user-supplied content by the affected software. An attacker could exploit these vulnerabilities by sending a malicious serialized Java object to a specific listener on an affected system. A successful exploit could allow the attacker to execute arbitrary commands on the device with the privileges of NT AUTHORITY\SYSTEM on the Windows target host. Cisco has not released software updates that address these vulnerabilities.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16970	Azure Sphere Unsigned Code Execution Vulnerability	8.1	More Details
CVE-2020-25694	A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If a client application that creates additional database connections only reuses the basic connection parameters while dropping security-relevant parameters, an opportunity for a man-in-the-middle attack, or the ability to observe clear-text transmissions, could exist. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.1	More Details
CVE-2020-27385	Incorrect Access Control in the FileEditor (/Admin/Views/FileEditor/) in FlexDotnetCMS before v1.5.11 allows an authenticated remote attacker to read and write to existing files outside the web root. The files can be accessed via directory traversal, i.e., by entering a .. (dot dot) path such as ..\..\..\..\..\<file> in the input field of the FileEditor. In FlexDotnetCMS before v1.5.8, it is also possible to access files by specifying the full path (e.g., C:\<file>). The files can then be edited via the FileEditor.	8.1	More Details
CVE-2020-14389	It was found that Keycloak before version 12.0.0 would permit a user with only view-profile role to manage the resources in the new account console, allowing access and modification of data the user was not intended to have.	8.1	More Details
CVE-2020-8259	Insufficient protection of the server-side encryption keys in Nextcloud Server 19.0.1 allowed an attacker to replace the encryption keys.	8.1	More Details
CVE-2020-17016	Microsoft SharePoint Server Spoofing Vulnerability	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26216	TYPO3 Fluid before versions 2.0.8, 2.1.7, 2.2.4, 2.3.7, 2.4.4, 2.5.11 and 2.6.10 is vulnerable to Cross-Site Scripting. Three XSS vulnerabilities have been detected in Fluid: 1. TagBasedViewHelper allowed XSS through maliciously crafted additionalAttributes arrays by creating keys with attribute-closing quotes followed by HTML. When rendering such attributes, TagBuilder would not escape the keys. 2. ViewHelpers which used the CompileWithContentArgumentAndRenderStatic trait, and which declared escapeOutput = false, would receive the content argument in unescaped format. 3. Subclasses of AbstractConditionViewHelper would receive the then and else arguments in unescaped format. Update to versions 2.0.8, 2.1.7, 2.2.4, 2.3.7, 2.4.4, 2.5.11 or 2.6.10 of this typo3fluid/fluid package that fix the problem described. More details are available in the linked advisory.	8.0	More Details
CVE-2020-26217	XStream before version 1.4.14 is vulnerable to Remote Code Execution.The vulnerability may allow a remote attacker to run arbitrary shell commands only by manipulating the processed input stream. Only users who rely on blocklists are affected. Anyone using XStream's Security Framework allowlist is not affected. The linked advisory provides code workarounds for users who cannot upgrade. The issue is fixed in version 1.4.14.	8.0	More Details
CVE-2020-26218	touchbase.ai before version 2.0 is vulnerable to Cross-Site Scripting. The vulnerability allows an attacker to inject HTML payloads which could result in defacement, user redirection to a malicious webpage/website etc. The issue is patched in version 2.0.	8.0	More Details
CVE-2020-26221	touchbase.ai before version 2.0 is vulnerable to Cross-Site Scripting (XSS). The vulnerability allows an attacker to send malicious JavaScript code which could result in hijacking of the user's cookie/session tokens, redirecting the user to a malicious webpage and performing unintended browser action. The issue is patched in version 2.0.	8.0	More Details
CVE-2020-17107	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17110	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17109	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17108	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17106	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2019-11121	Improper file permissions in the installer for the Intel(R) Media SDK for Windows before version 2019 R1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17105	AV1 Video Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17104	Visual Studio Code JSHint Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-12306	Incorrect default permissions in the Intel(R) RealSense(TM) D400 Series Dynamic Calibration Tool before version 2.11, may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17101	HEIF Image Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-8760	Integer overflow in subsystem for Intel(R) AMT versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 14.0.45 may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17091	Microsoft Teams Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-12304	Improper access control in Installer for Intel(R) DAL SDK before version 2.1 for Windows may allow an authenticated user to potentially enable escalation of privileges via local access.	7.8	More Details
CVE-2020-17088	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17087	Windows Kernel Local Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17086	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-0590	Improper input validation in BIOS firmware for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-12307	Improper permissions in some Intel(R) High Definition Audio drivers before version 9.21.00.4561 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-11201	Arbitrary access to DSP memory due to improper check in loaded library for data received from CPU side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCM6125, QCS410, QCS603, QCS605, QCS610, QCS6125, SA6145P, SA6155, SA6155P, SA8155, SA8155P, SDA640, SDA845, SDM640, SDM830, SDM845, SDX50M, SDX55, SDX55M, SM6125, SM6150, SM6250, SM6250P, SM7125, SM7150, SM7150P, SM8150, SM8150P	7.8	More Details
CVE-2020-8750	Use after free in Kernel Mode Driver for Intel(R) TXE versions before 3.1.80 and 4.0.30 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-11206	Possible buffer overflow in Fastrpc while handling received parameters due to lack of validation on input parameters' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, MSM8998, QCM4290, QCM6125, QCS410, QCS4290, QCS610, QCS6125, QSM8250, QSM8350, SA6145P, SA6150P, SA6155, SA6155P, SA8150P, SA8155, SA8155P, SA8195P, SC7180, SDA640, SDA660, SDA845, SDA855, SDM640, SDM660, SDM830, SDM845, SDM850, SDX50M, SDX55, SDX55M, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6150, SM6150P, SM6250, SM6250P, SM6350, SM7125, SM7150, SM7150P, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SM8350, SM8350P, SXR2130, SXR2130P	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11175	u'Use after free issue in Bluetooth transport driver when a method in the object is accessed after the object has been deleted due to improper timer handling.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009W, MSM8909W, QCS605, QM215, SA6155, SA6155P, SA8155, SA8155P, SDA640, SDA670, SDA855, SDM1000, SDM640, SDM670, SDM710, SDM845, SDX50M, SDX55, SDX55M, SM6125, SM6350, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SXR1120, SXR1130, SXR2130, SXR2130P	7.8	More Details
CVE-2020-11202	Buffer overflow/underflow occurs when typecasting the buffer passed by CPU internally in the library which is not aligned with the actual size of the structure' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCM6125, QCS410, QCS603, QCS605, QCS610, QCS6125, SA6145P, SA6155, SA6155P, SA8155, SA8155P, SDA640, SDA670, SDA845, SDM640, SDM670, SDM710, SDM830, SDM845, SDX50M, SDX55, SDX55M, SM6125, SM6150, SM6150P, SM6250, SM6250P, SM7125, SM7150, SM7150P, SM8150, SM8150P	7.8	More Details
CVE-2020-11131	u'Possible buffer overflow in WMA message processing due to integer overflow occurs when processing command received from user space' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9250, MDM9628, MDM9640, MDM9650, MSM8996AU, QCS405, SDA845, SDX20, SDX20M, WCD9330	7.8	More Details
CVE-2020-11130	u'Possible buffer overflow in WIFI hal process due to copying data without checking the buffer length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile in QCM4290, QCS4290, QM215, QSM8350, SA6145P, SA6155, SA6155P, SA8155, SA8155P, SC8180X, SC8180XP, SDX55, SDX55M, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6250, SM6350, SM7125, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SM8350, SM8350P, SXR2130, SXR2130P	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11127	u'Integer overflow can cause a buffer overflow due to lack of table length check in the extensible boot Loader during the validation of security metadata while processing objects to be loaded' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCM4290, QCS405, QCS410, QCS4290, QCS610, QSM8250, SA415M, SA515M, SA6145P, SA6150P, SA6155, SA6155P, SA8150P, SA8155, SA8155P, SA8195P, SC7180, SC8180X, SC8180X+SDX55, SC8180XP, SDA640, SDA845, SDA855, SDM1000, SDM640, SDM830, SDM845, SDM850, SDX24, SDX50M, SDX55, SDX55M, SM4125, SM4250, SM4250P, SM6115, SM6115P, SM6150, SM6150P, SM6250, SM6250P, SM6350, SM7125, SM7150, SM7150P, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SXR2130, SXR2130P	7.8	More Details
CVE-2020-15481	An issue was discovered in PassMark BurnInTest v9.1 Build 1008, OSForensics v7.1 Build 1012, and PerformanceTest v10.0 Build 1008. The kernel driver exposes IOCTL functionality that allows low-privilege users to map arbitrary physical memory into the address space of the calling process. This could lead to arbitrary Ring-0 code execution and escalation of privileges. This affects DirectIo32.sys and DirectIo64.sys drivers. This issue is fixed in BurnInTest v9.2, PerformanceTest v10.0 Build 1009, OSForensics v8.0.	7.8	More Details
CVE-2020-17082	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-11121	u'Possible buffer overflow in WIFI hal process due to usage of memcpy without checking length of destination buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile in QCM4290, QCS4290, QM215, QSM8350, SA6145P, SA6155, SA6155P, SA8155, SA8155P, SC8180X, SC8180XP, SDX55, SDX55M, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6250, SM6350, SM7125, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SM8350, SM8350P, SXR2130, SXR2130P	7.8	More Details
CVE-2020-11205	u'Possible integer overflow to heap overflow while processing command due to lack of check of packet length received' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile in QSM8350, SA6145P, SA6150P, SA6155, SA6155P, SA8150P, SA8155P, SA8195P, SDX55M, SM8250, SM8350, SM8350P, SXR2130, SXR2130P	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12354	Incorrect default permissions in Windows(R) installer in Intel(R) AMT SDK versions before 14.0.0.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-8744	Improper initialization in subsystem for Intel(R) CSME versions before12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25, Intel(R) TXE versions before 4.0.30 Intel(R) SPS versions before E3_05.01.04.200 may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-11207	Buffer overflow in LibFastCV library due to improper size checks with respect to buffer length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8052, APQ8056, APQ8076, APQ8096, APQ8096SG, APQ8098, MDM9655, MSM8952, MSM8956, MSM8976, MSM8976SG, MSM8996, MSM8996SG, MSM8998, QCM4290, QCM6125, QCS410, QCS4290, QCS610, QCS6125, QSM8250, SA6145P, SA6150P, SA6155, SA6155P, SA8150P, SA8155, SA8155P, SA8195P, SC7180, SDA640, SDA660, SDA845, SDA855, SDM640, SDM660, SDM830, SDM845, SDM850, SDX50M, SDX55, SDX55M, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6150, SM6150P, SM6250, SM6250P, SM6350, SM7125, SM7150, SM7150P, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SXR2130, SXR2130P	7.8	More Details
CVE-2020-5796	Improper preservation of permissions in Nagios XI 5.7.4 allows a local, low-privileged, authenticated user to weaken the permissions of files, resulting in low-privileged users being able to write to and execute arbitrary PHP code with root privileges.	7.8	More Details
CVE-2020-13770	Several services are accessing named pipes in Ivanti Endpoint Manager through 2020.1.1 with default or overly permissive security attributes; as these services run as user ‘NT AUTHORITY\SYSTEM’, the issue can be used to escalate privileges from a local standard or service account having SeImpersonatePrivilege (eg. user ‘NT AUTHORITY\NETWORK SERVICE’).	7.8	More Details
CVE-2020-13771	Various components in Ivanti Endpoint Manager through 2020.1.1 rely on Windows search order when loading a (nonexistent) library file, allowing (under certain conditions) one to gain code execution (and elevation of privileges to the level of privilege held by the vulnerable component such as NT AUTHORITY\SYSTEM) via DLL hijacking. This affects ldiscn32.exe, IpmiRedirectionService.exe, LDAPWhoAmI.exe, and ldprofile.exe.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5992	NVIDIA GeForce NOW application software on Windows, all versions prior to 2.0.25.119, contains a vulnerability in its open-source software dependency in which the OpenSSL library is vulnerable to binary planting attacks by a local user, which may lead to code execution or escalation of privileges.	7.8	More Details
CVE-2020-11208	Out of Bound issue in DSP services while processing received arguments due to improper validation of length received as an argument' in SD820, SD821, SD820, QCS603, QCS605, SDA855, SA6155P, SA6145P, SA6155, SA6155P, SD855, SD 675, SD660, SD429, SD439	7.8	More Details
CVE-2020-3632	u'Incorrect validation of ring context fetched from host memory can lead to memory overflow' in Snapdragon Compute, Snapdragon Mobile in QSM8350, SC7180, SDX55, SDX55M, SM6150, SM6250, SM6250P, SM7125, SM7150, SM7150P, SM7250, SM7250P, SM8150, SM8150P, SM8250, SM8350, SM8350P, SXR2130, SXR2130P	7.8	More Details
CVE-2020-7331	Unquoted service executable path in McAfee Endpoint Security (ENS) prior to 10.7.0 November 2020 Update allows local users to cause a denial of service and malicious file execution via carefully crafted and named executable files.	7.8	More Details
CVE-2020-8739	Use of potentially dangerous function in Intel BIOS platform sample code for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-12318	Protection mechanism failure in some Intel(R) PROSet/Wireless WiFi products before version 21.110 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17075	Windows USO Core Worker Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-27192	BinaryNights ForkLift 3.4 was compiled with the com.apple.security.cs.disable-library-validation flag enabled which allowed a local attacker to inject code into ForkLift. This would allow the attacker to run malicious code with escalated privileges through ForkLift's helper tool.	7.8	More Details
CVE-2020-17014	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17019	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-12335	Improper permissions in the installer for the Intel(R) Processor Identification Utility before version 6.4.0603 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17024	Windows Client Side Rendering Print Provider Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17025	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17026	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17027	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17028	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-12334	Improper permissions in the installer for the Intel(R) Advisor tools before version 2020 Update 2 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17031	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17032	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17033	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17034	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17035	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17079	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17037	Windows WalletService Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-12336	Insecure default variable initialization in firmware for some Intel(R) NUCs may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-12345	Improper permissions in the installer for the Intel(R) Data Center Manager Console before version 3.6.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-12333	Insufficiently protected credentials in the Intel(R) QAT for Linux before version 1.7.l.4.10.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17012	Windows Bind Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-12927	A potential vulnerability in a dynamically loaded AMD driver in AMD VBIOS Flash Tool SDK may allow any authenticated user to escalate privileges to NT authority system.	7.8	More Details
CVE-2020-6147	A heap overflow vulnerability exists in Pixar OpenUSD 20.05 when the software parses compressed sections in binary USD files. This instance exists in the USDC file format FIELDS section decompression heap overflow.	7.8	More Details
CVE-2020-6148	A heap overflow vulnerability exists in Pixar OpenUSD 20.05 when the software parses compressed sections in binary USD files. An instance exists in USDC file format FIELDSETS section decompression heap overflow.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24525	Insecure inherited permissions in firmware update tool for some Intel(R) NUCs may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-6149	A heap overflow vulnerability exists in Pixar OpenUSD 20.05 when the software parses compressed sections in binary USD files. To trigger this vulnerability, the victim needs to open an attacker-provided malformed file in an instance in USDC file format PATHS section.	7.8	More Details
CVE-2020-24456	Incorrect default permissions in the Intel(R) Board ID Tool version v.1.01 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-16273	In Arm software implementing the Armv8-M processors (all versions), the stack selection mechanism could be influenced by a stack-underflow attack in v8-M TrustZone based processors. An attacker can cause a change to the stack pointer used by the Secure World from a non-secure application if the stack is not initialized. This vulnerability affects only the software that is based on Armv8-M processors with the Security Extension.	7.8	More Details
CVE-2020-6150	A heap overflow vulnerability exists in Pixar OpenUSD 20.05 when the software USDC file format SPECS section decompression heap overflow.	7.8	More Details
CVE-2020-12350	Improper access control in the Intel(R) XTU before version 6.5.1.360 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17001	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-13958	A vulnerability in Apache OpenOffice scripting events allows an attacker to construct documents containing hyperlinks pointing to an executable on the target users file system. These hyperlinks can be triggered unconditionally. In fixed versions no internal protocol may be called from the document event handler and other hyperlinks require a control-click.	7.8	More Details
CVE-2020-6155	A heap overflow vulnerability exists in the Pixar OpenUSD 20.05 while parsing compressed value rep arrays in binary USD files. A specially crafted malformed file can trigger a heap overflow, which can result in remote code execution. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12346	Improper permissions in the installer for the Intel(R) Battery Life Diagnostic Tool before version 1.0.7 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17010	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17011	Windows Port Class Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17038	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-12303	Use after free in DAL subsystem for Intel(R) CSME versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25, Intel(R) TXE 3.1.80, 4.0.30 may allow an authenticated user to potentially enable escalation of privileges via local access.	7.8	More Details
CVE-2020-17055	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17067	Microsoft Excel Security Feature Bypass Vulnerability	7.8	More Details
CVE-2020-17066	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17065	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17064	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-12297	Improper access control in Installer for Intel(R) CSME Driver for Windows versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25, Intel TXE 3.1.80, 4.0.30 may allow an authenticated user to potentially enable escalation of privileges via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12320	Uncontrolled search path in Intel(R) SCS Add-on for Microsoft* SCCM before version 2.1.10 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17062	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-12324	Protection mechanism failure in some Intel(R) Thunderbolt(TM) DCH drivers for Windows* before version 72 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-12325	Improper buffer restrictions in some Intel(R) Thunderbolt(TM) DCH drivers for Windows* before version 72 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-17068	Windows GDI+ Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-6156	A heap overflow vulnerability exists in Pixar OpenUSD 20.05 when the software parses compressed sections in binary USD files. To trigger this vulnerability, the victim needs to open an attacker-provided malformed file in an instance USDC file format path element token index.	7.8	More Details
CVE-2020-17076	Windows Update Orchestrator Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17077	Windows Update Stack Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-12329	Uncontrolled search path in the Intel(R) VTune(TM) Profiler before version 2020 Update 1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-12330	Improper permissions in the installer for the Intel(R) Falcon 8+ UAS AscTec Thermal Viewer, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-12331	Improper access controls in Intel Unite(R) Cloud Service client before version 4.2.12212 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17073	Windows Update Orchestrator Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-12332	Improper permissions in the installer for the Intel(R) HID Event Filter Driver, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-15349	BinaryNights ForkLift 3.x before 3.4 has a local privilege escalation vulnerability because the privileged helper tool implements an XPC interface that allows file operations to any process (copy, move, delete) as root and changing permissions.	7.8	More Details
CVE-2020-17044	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17078	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17070	Windows Update Medic Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17043	Windows Remote Access Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17041	Windows Print Configuration Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17074	Windows Update Orchestrator Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-16997	Remote Desktop Protocol Server Information Disclosure Vulnerability	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26223	Spree is a complete open source e-commerce solution built with Ruby on Rails. In Spree from version 3.7 and before versions 3.7.13, 4.0.5, and 4.1.12, there is an authorization bypass vulnerability. The perpetrator could query the API v2 Order Status endpoint with an empty string passed as an Order token. This is patched in versions 3.7.11, 4.0.4, or 4.1.11 depending on your used Spree version. Users of Spree < 3.7 are not affected.	7.7	More Details
CVE-2020-5666	Uncontrolled resource consumption vulnerability in MELSEC iQ-R Series CPU Modules (R00/01/02CPU Firmware versions from '05' to '19' and R04/08/16/32/120(EN)CPU Firmware versions from '35' to '51') allows a remote attacker to cause an error in a CPU unit via a specially crafted HTTP packet, which may lead to a denial-of-service (DoS) condition in execution of the program and its communication.	7.5	More Details
CVE-2020-1847	There is a denial of service vulnerability in some Huawei products. There is no protection against the attack scenario of specific protocol. A remote, unauthorized attackers can construct attack scenarios, which leads to denial of service.Affected product versions include:NIP6300 versions V500R001C30,V500R001C60;NIP6600 versions V500R001C30,V500R001C60;Secospace USG6300 versions V500R001C30,V500R001C60;Secospace USG6500 versions V500R001C30,V500R001C60;Secospace USG6600 versions V500R001C30,V500R001C60;USG9500 versions V500R001C30,V500R001C60.	7.5	More Details
CVE-2020-24454	Improper Restriction of XML External Entity Reference in subsystem forIntel(R) Quartus(R) Prime Pro Edition before version 20.3 and Intel(R) Quartus(R) Prime Standard Edition before version 20.2 may allow unauthenticated user to potentially enable information disclosure via network access.	7.5	More Details
CVE-2020-27217	In Eclipse Hono version 1.3.0 and 1.4.0 the AMQP protocol adapter does not verify the size of AMQP messages received from devices. In particular, a device may send messages that are bigger than the max-message-size that the protocol adapter has indicated during link establishment. While the AMQP 1.0 protocol explicitly disallows a peer to send such messages, a hand crafted AMQP 1.0 client could exploit this behavior in order to send a message of unlimited size to the adapter, eventually causing the adapter to fail with an out of memory exception.	7.5	More Details
CVE-2020-7772	This affects the package doc-path before 2.1.2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25155	The affected product transmits unencrypted sensitive information, which may allow an attacker to access this information on the NIO 50 (all versions).	7.5	More Details
CVE-2020-25151	The affected product does not properly validate input, which may allow an attacker to execute a denial-of-service attack on the NIO 50 (all versions).	7.5	More Details
CVE-2020-28268	Prototype pollution vulnerability in 'controlled-merge' versions 1.0.0 through 1.2.0 allows attacker to cause a denial of service and may lead to remote code execution.	7.5	More Details
CVE-2020-24573	BAB TECHNOLOGIE GmbH eibPort V3 prior to 3.8.3 devices allow denial of service (Uncontrolled Resource Consumption) via requests to the lighttpd component.	7.5	More Details
CVE-2020-8754	Out-of-bounds read in subsystem for Intel(R) AMT, Intel(R) ISM versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70 and 14.0.45 may allow an unauthenticated user to potentially enable information disclosure via network access.	7.5	More Details
CVE-2020-8753	Out-of-bounds read in DHCP subsystem for Intel(R) AMT, Intel(R) ISM versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70 and 14.0.45 may allow an unauthenticated user to potentially enable information disclosure via network access.	7.5	More Details
CVE-2020-6019	Valve's Game Networking Sockets prior to version v1.2.0 improperly handles inlined statistics messages in function CConnectionTransportUDPBase::Received_Data(), leading to an exception thrown from libprotobuf and resulting in a crash.	7.5	More Details
CVE-2020-8583	Element Software versions prior to 12.2 and HCI versions prior to 1.8P1 are susceptible to a vulnerability which could allow an attacker to discover sensitive information by intercepting its transmission within an https session.	7.5	More Details
CVE-2020-25165	BD Alaris PC Unit, Model 8015, Versions 9.33.1 and earlier and BD Alaris Systems Manager, Versions 4.33 and earlier The affected products are vulnerable to a network session authentication vulnerability within the authentication process between specified versions of the BD Alaris PC Unit and the BD Alaris Systems Manager. If exploited, an attacker could perform a denial-of-service attack on the BD Alaris PC Unit by modifying the configuration headers of data in transit. A denial-of-service attack could lead to a drop in the wireless capability of the BD Alaris PC Unit, resulting in manual operation of the PC Unit.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15783	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC TDC CPU555 (All versions), SINUMERIK 840D sl (All versions). Sending multiple specially crafted packets to the affected devices could cause a Denial-of-Service on port 102. A cold restart is required to recover the service.	7.5	More Details
CVE-2020-26224	In PrestaShop before version 1.7.6.9 an attacker is able to list all the orders placed on the website without being logged by abusing the function that allows a shopping cart to be recreated from an order already placed. The problem is fixed in 1.7.6.9.	7.5	More Details
CVE-2020-25209	In JetBrains YouTrack before 2020.3.6638, improper access control for some subresources leads to information disclosure via the REST API.	7.5	More Details
CVE-2020-27553	In BASETech GE-131 BT-1837836 firmware 20180921, the web-server on the system is configured with the option “DocumentRoot /etc“. This allows an attacker with network access to the web-server to download any files from the “/etc” folder without authentication. No path traversal sequences are needed to exploit this vulnerability.	7.5	More Details
CVE-2020-7768	The package grpc before 1.24.4; the package @grpc/grpc-js before 1.1.8 are vulnerable to Prototype Pollution via loadPackageDefinition.	7.5	More Details
CVE-2020-4476	IBM Sterling File Gateway 2.2.0.0 through 2.2.6.5 and 6.0.0.0 through 6.0.3.2 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: 181778.	7.5	More Details
CVE-2020-27523	Solstice-Pod up to 5.0.2 WEBRTC server mishandles the format-string specifiers %x; %p; %c and %s in the screen_key, display_name, browser_name, and operation_system parameter during the authentication process. This may crash the server and force Solstice-Pod to reboot, which leads to a denial of service.	7.5	More Details
CVE-2020-27554	Cleartext Transmission of Sensitive Information vulnerability in BASETech GE-131 BT-1837836 firmware 20180921 exists which could leak sensitive information transmitted between the mobile app and the camera device.	7.5	More Details
CVE-2020-25400	Cross domain policies in Taskcafe Project Management tool before version 0.1.0 and 0.1.1 allows remote attackers to access sensitive data such as access token.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28723	Memory leak in IPv6Param::setAddress in CloudAvid PParam 1.3.1.	7.5	More Details
CVE-2020-17047	Windows Network File System Denial of Service Vulnerability	7.5	More Details
CVE-2020-23490	There was a local file disclosure vulnerability in AVideo < 8.9 via the proxy streaming. An unauthenticated attacker can exploit this issue to read an arbitrary file on the server. Which could leak database credentials or other sensitive information such as /etc/passwd file.	7.5	More Details
CVE-2020-16992	Azure Sphere Elevation of Privilege Vulnerability	7.5	More Details
CVE-2020-27623	JetBrains IdeaVim before version 0.58 might have caused an information leak in limited circumstances.	7.5	More Details
CVE-2020-27191	LionWiki before 3.2.12 allows an unauthenticated user to read files as the web server user via crafted string in the index.php f1 variable, aka Local File Inclusion. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.5	More Details
CVE-2020-2022	An information exposure vulnerability exists in Palo Alto Networks Panorama software that discloses the token for the Panorama web interface administrator's session to a managed device when the Panorama administrator performs a context switch into that device. This vulnerability allows an attacker to gain privileged access to the Panorama web interface. An attacker requires some knowledge of managed firewalls to exploit this issue. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.17; PAN-OS 9.0 versions earlier than PAN-OS 9.0.11; PAN-OS 9.1 versions earlier than PAN-OS 9.1.5.	7.5	More Details
CVE-2020-17052	Scripting Engine Memory Corruption Vulnerability	7.5	More Details
CVE-2020-27423	Anuko Time Tracker v1.19.23.5311 lacks rate limit on the password reset module which allows attacker to perform Denial of Service attack on any legitimate user's mailbox	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25658	It was found that python-rsa is vulnerable to Bleichenbacher timing attacks. An attacker can use this flaw via the RSA decryption API to decrypt parts of the cipher text encrypted with RSA.	7.5	More Details
CVE-2020-25013	JetBrains ToolBox before version 1.18 is vulnerable to a Denial of Service attack via a browser protocol handler.	7.5	More Details
CVE-2020-26552	An issue was discovered in Aviatrix Controller before R6.0.2483. Multiple executable files, that implement API endpoints, do not require a valid session ID for access.	7.5	More Details
CVE-2020-26551	An issue was discovered in Aviatrix Controller before R5.3.1151. Encrypted key values are stored in a readable file.	7.5	More Details
CVE-2020-26550	An issue was discovered in Aviatrix Controller before R5.3.1151. An encrypted file containing credentials to unrelated systems is protected by a three-character key.	7.5	More Details
CVE-2019-17566	Apache Batik is vulnerable to server-side request forgery, caused by improper input validation by the "xlink:href" attributes. By using a specially-crafted argument, an attacker could exploit this vulnerability to cause the underlying server to make arbitrary GET requests.	7.5	More Details
CVE-2020-26549	An issue was discovered in Aviatrix Controller before R5.4.1290. The htaccess protection mechanism to prevent requests to directories can be bypassed for file downloading.	7.5	More Details
CVE-2020-8272	Authentication Bypass resulting in exposure of SD-WAN functionality in Citrix SD-WAN Center versions before 11.2.2, 11.1.2b and 10.2.8	7.5	More Details
CVE-2020-17053	Internet Explorer Memory Corruption Vulnerability	7.5	More Details
CVE-2020-17058	Microsoft Browser Memory Corruption Vulnerability	7.5	More Details
CVE-2020-26509	Airleader Master and Easy <= 6.21 devices have default credentials that can be used for a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26230	Radar COVID is the official COVID-19 exposure notification app for Spain. In affected versions of Radar COVID, identification and de-anonymization of COVID-19 positive users that upload Radar COVID TEKs to the Radar COVID server is possible. This vulnerability enables the identification and de-anonymization of COVID-19 positive users when using Radar COVID. The vulnerability is caused by the fact that Radar COVID connections to the server (uploading of TEKs to the backend) are only made by COVID-19 positives. Therefore, any on-path observer with the ability to monitor traffic between the app and the server can identify which users had a positive test. Such an adversary can be the mobile network operator (MNO) if the connection is done through a mobile network, the Internet Service Provider (ISP) if the connection is done through the Internet (e.g., a home network), a VPN provider used by the user, the local network operator in the case of enterprise networks, or any eavesdropper with access to the same network (WiFi or Ethernet) as the user as could be the case of public WiFi hotspots deployed at shopping centers, airports, hotels, and coffee shops. The attacker may also de-anonymize the user. For this additional stage to succeed, the adversary needs to correlate Radar COVID traffic to other identifiable information from the victim. This could be achieved by associating the connection to a contract with the name of the victim or by associating Radar COVID traffic to other user-generated flows containing identifiers in the clear (e.g., HTTP cookies or other mobile flows sending unique identifiers like the IMEI or the AAID without encryption). The former can be executed, for instance, by the Internet Service Provider or the MNO. The latter can be executed by any on-path adversary, such as the network provider or even the cloud provider that hosts more than one service accessed by the victim. The farther the adversary is either from the victim (the client) or the end-point (the server), the less likely it may be that the adversary has access to re-identification information. The vulnerability has been mitigated with the injection of dummy traffic from the application to the backend. Dummy traffic is generated by all users independently of whether they are COVID-19 positive or not. The issue was fixed in iOS in version 1.0.8 (uniform distribution), 1.1.0 (exponential distribution), Android in version 1.0.7 (uniform distribution), 1.1.0 (exponential distribution), Backend in version 1.1.2-RELEASE. For more information see the referenced GitHub Security Advisory.	7.4	More Details
CVE-2020-27125	A vulnerability in Cisco Security Manager could allow an unauthenticated, remote attacker to access sensitive information on an affected system. The vulnerability is due to insufficient protection of static credentials in the affected software. An attacker could exploit this vulnerability by viewing source code. A successful exploit could allow the attacker to view static credentials, which the attacker could use to carry out further attacks.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25705	A flaw in ICMP packets in the Linux kernel may allow an attacker to quickly scan open UDP ports. This flaw allows an off-path remote attacker to effectively bypass source port UDP randomization. Software that relies on UDP source port randomization are indirectly affected as well on the Linux Based Products (RUGGEDCOM RM1224: All versions between v5.0 and v6.4, SCALANCE M-800: All versions between v5.0 and v6.4, SCALANCE S615: All versions between v5.0 and v6.4, SCALANCE SC-600: All versions prior to v2.1.3, SCALANCE W1750D: v8.3.0.1, v8.6.0, and v8.7.0, SIMATIC Cloud Connect 7: All versions, SIMATIC MV500 Family: All versions, SIMATIC NET CP 1243-1 (incl. SIPLUS variants): Versions 3.1.39 and later, SIMATIC NET CP 1243-7 LTE EU: Version	7.4	More Details
CVE-2020-7774	The package y18n before 3.2.2, 4.0.1 and 5.0.5, is vulnerable to Prototype Pollution.	7.3	More Details
CVE-2020-16984	Azure Sphere Unsigned Code Execution Vulnerability	7.3	More Details
CVE-2020-16994	Azure Sphere Unsigned Code Execution Vulnerability	7.3	More Details
CVE-2020-16991	Azure Sphere Unsigned Code Execution Vulnerability	7.3	More Details
CVE-2020-16987	Azure Sphere Unsigned Code Execution Vulnerability	7.3	More Details
CVE-2020-2490	If exploited, the command injection vulnerability could allow remote attackers to execute arbitrary commands. This issue affects: QNAP Systems Inc. QTS versions prior to 4.4.3.1421 on build 20200907.	7.2	More Details
CVE-2020-2492	If exploited, the command injection vulnerability could allow remote attackers to execute arbitrary commands. This issue affects: QNAP Systems Inc. QTS versions prior to 4.4.3.1421 on build 20200907.	7.2	More Details
CVE-2020-28692	In Gila CMS 1.16.0, an attacker can upload a shell to tmp directy and abuse .htaccess through the logs function for executing PHP files.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26805	In Sentrifugo 3.2, admin can edit employee's informations via this endpoint --> /sentrifugo/index.php/empadditionaldetails/edit/userid/2. In this POST request, "employeeNumId" parameter is affected by SQLi vulnerability. Attacker can inject SQL commands into query, read data from database or write data into the database.	7.2	More Details
CVE-2020-21665	In fastadmin V1.0.0.20191212_beta, when a user with administrator rights has logged in, a malicious parameter can be passed for SQL injection in URL /admin/ajax/weigh.	7.2	More Details
CVE-2020-7328	External entity attack vulnerability in the ePO extension in McAfee MVISION Endpoint prior to 20.11 allows remote attackers to gain control of a resource or trigger arbitrary code execution via improper input validation of an HTTP request, where the content for the attack has been loaded into ePO by an ePO administrator.	7.2	More Details
CVE-2020-21667	In fastadmin-tp6 v1.0, in the file app/admin/controller/Ajax.php the 'table' parameter passed is not filtered so a malicious parameter can be passed for SQL injection.	7.2	More Details
CVE-2020-4685	A low level user of IBM Cognos Controller 10.3.0, 10.3.1, 10.4.0, 10.4.1, and 10.4.2 who has Administration rights to the server where the application is installed, can escalate their privilege from Low level to Super Admin and gain access to Create/Update/Delete any level of user in Cognos Controller. IBM X-Force ID: 186625.	7.2	More Details
CVE-2020-2000	An OS command injection and memory corruption vulnerability in the PAN-OS management web interface that allows authenticated administrators to disrupt system processes and potentially execute arbitrary code and OS commands with root privileges. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.4; PAN-OS 10.0 versions earlier than PAN-OS 10.0.1.	7.2	More Details
CVE-2020-7329	Server-side request forgery vulnerability in the ePO extension in McAfee MVISION Endpoint prior to 20.11 allows remote attackers trigger server-side DNS requests to arbitrary domains via carefully constructed XML files loaded by an ePO administrator.	7.2	More Details
CVE-2020-28914	An improper file permissions vulnerability affects Kata Containers prior to 1.11.5. When using a Kubernetes hostPath volume and mounting either a file or directory into a container as readonly, the file/directory is mounted as readOnly inside the container, but is still writable inside the guest. For a container breakout situation, a malicious guest can potentially modify or delete files/directories expected to be read-only.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26405	Path traversal vulnerability in package upload functionality in GitLab CE/EE starting from 12.8 allows an attacker to save packages in arbitrary locations. Affected versions are >=12.8, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.	7.1	More Details
CVE-2020-27524	On Audi A7 MMI 2014 vehicles, the Bluetooth stack in Audi A7 MMI Multiplayer with version (N+R_CN_AU_P0395) mishandles %x and %s format string specifiers in a device name. This may lead to memory content leaks and potentially crash the services.	7.1	More Details
CVE-2020-11132	u'Buffer over read in boot due to size check ignored before copying GUID attribute from request to response' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096AU, APQ8098, MDM8207, MDM9150, MDM9205, MDM9206, MDM9207, MDM9250, MDM9607, MDM9628, MDM9650, MSM8108, MSM8208, MSM8209, MSM8608, MSM8905, MSM8909, MSM8998, QCM4290, QCS405, QCS410, QCS4290, QCS603, QCS605, QCS610, QSM8250, SA415M, SA515M, SA6145P, SA6150P, SA6155, SA6155P, SA8150P, SA8155, SA8155P, SA8195P, SC7180, SC8180X, SC8180X+SDX55, SC8180XP, SDA640, SDA670, SDA845, SDA855, SDM1000, SDM640, SDM670, SDM710, SDM712, SDM830, SDM845, SDM850, SDX24, SDX50M, SDX55, SDX55M, SM4125, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6150, SM6150P, SM6250, SM6250P, SM6350, SM7125, SM7150, SM7150P, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SXR1120, SXR1130, SXR2130, SXR2130P, WCD9330	7.1	More Details
CVE-2020-16998	DirectX Elevation of Privilege Vulnerability	7.0	More Details
CVE-2020-17007	Windows Error Reporting Elevation of Privilege Vulnerability	7.0	More Details
CVE-2020-17057	Windows Win32k Elevation of Privilege Vulnerability	7.0	More Details
CVE-2020-7332	Cross Site Request Forgery vulnerability in the firewall ePO extension of McAfee Endpoint Security (ENS) prior to 10.7.0 November 2020 Update allows an attacker to execute arbitrary HTML code due to incorrect security configuration.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16988	Azure Sphere Elevation of Privilege Vulnerability	6.9	More Details
CVE-2020-12355	Authentication bypass by capture-replay in RPMB protocol message authentication subsystem in Intel(R) TXE versions before 4.0.30 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2020-8705	Insecure default initialization of resource in Intel(R) Boot Guard in Intel(R) CSME versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25, Intel(R) TXE versions before 3.1.80 and 4.0.30, Intel(R) SPS versions before E5_04.01.04.400, E3_04.01.04.200, SoC-X_04.00.04.200 and SoC-A_04.00.04.300 may allow an unauthenticated user to potentially enable escalation of privileges via physical access.	6.8	More Details
CVE-2020-17063	Microsoft Office Online Spoofing Vulnerability	6.8	More Details
CVE-2020-28656	The update functionality of the Discover Media infotainment system in Volkswagen Polo 2019 vehicles allows physically proximate attackers to execute arbitrary code because some unsigned parts of a metainfo file are parsed, which can cause attacker-controlled files to be written to the infotainment system and executed as root.	6.8	More Details
CVE-2020-12312	Improper buffer restrictions in the Intel(R) Stratix(R) 10 FPGA firmware provided with the Intel(R) Quartus(R) Prime Pro software before version 20.2 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2020-8737	Improper buffer restrictions in the Intel(R) Stratix(R) 10 FPGA firmware provided with the Intel(R) Quartus(R) Prime Pro software before version 20.1 may allow an unauthenticated user to potentially enable escalation of privilege and/or information disclosure via physical access.	6.8	More Details
CVE-2020-8745	Insufficient control flow management in subsystem for Intel(R) CSME versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25 , Intel(R) TXE versions before 3.1.80 and 4.0.30 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2020-12337	Improper buffer restrictions in firmware for some Intel(R) NUCs may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9127	Some Huawei products have a command injection vulnerability. Due to insufficient input validation, an attacker with high privilege may inject some malicious codes in some files of the affected products. Successful exploit may cause command injection.Affected product versions include:NIP6300 versions V500R001C30,V500R001C60;NIP6600 versions V500R001C30,V500R001C60;Secospace USG6300 versions V500R001C30,V500R001C60;Secospace USG6500 versions V500R001C30,V500R001C60;Secospace USG6600 versions V500R001C30,V500R001C60;USG9500 versions V500R001C30,V500R001C60.	6.7	More Details
CVE-2020-0593	Improper buffer restrictions in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-9129	HUAWEI Mate 30 versions earlier than 10.1.0.159(C00E159R7P2) have a vulnerability of improper buffer operation. Due to improper restrictions, local attackers with high privileges can exploit the vulnerability to cause system heap overflow.	6.7	More Details
CVE-2020-0587	Improper conditions check in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-8690	Protection mechanism failure in Intel(R) Ethernet 700 Series Controllers before version 7.3 may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access.	6.7	More Details
CVE-2020-8691	A logic issue in the firmware of the Intel(R) Ethernet 700 Series Controllers may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access.	6.7	More Details
CVE-2020-8692	Insufficient access control in the firmware of the Intel(R) Ethernet 700 Series Controllers before version 7.3 may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access.	6.7	More Details
CVE-2020-8693	Improper buffer restrictions in the firmware of the Intel(R) Ethernet 700 Series Controllers may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access.	6.7	More Details
CVE-2020-8353	Prior to August 10, 2020, some Lenovo Desktop and Workstation systems were shipped with the Embedded Host Based Configuration (EHBC) feature of Intel AMT enabled. This could allow an administrative user with local access to configure Intel AMT.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12323	Improper input validation in the Intel(R) ADAS IE before version ADAS_IE_1.0.766 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-8738	Improper conditions check in Intel BIOS platform sample code for some Intel(R) Processors before may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-8676	Improper access control in the Intel(R) Visual Compute Accelerator 2, all versions, may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-8740	Out of bounds write in Intel BIOS platform sample code for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-0592	Out of bounds write in BIOS firmware for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access.	6.7	More Details
CVE-2020-8756	Improper input validation in subsystem for Intel(R) CSME versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70 and 14.0.45 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-8757	Out-of-bounds read in subsystem for Intel(R) AMT versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70 and 14.0.45 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-0588	Improper conditions check in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-0591	Improper buffer restrictions in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-8764	Improper access control in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-0572	Improper input validation in the firmware for Intel(R) Server Board S2600ST and S2600WF families may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0599	Improper access control in the PMC for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-17049	A security feature bypass vulnerability exists in the way Key Distribution Center (KDC) determines if a service ticket can be used for delegation via Kerberos Constrained Delegation (KCD). To exploit the vulnerability, a compromised service that is configured to use KCD could tamper with a service ticket that is not valid for delegation to force the KDC to accept it. The update addresses this vulnerability by changing how the KDC validates service tickets used with KCD.	6.6	More Details
CVE-2020-7773	This affects the package markdown-it-highlightjs before 3.3.1. It is possible insert malicious JavaScript as a value of lang in the markdown-it-highlightjs Inline code highlighting feature. const markdownItHighlightjs = require("markdown-it-highlightjs"); const md = require('markdown-it'); const reuslt_xss = md() .use(markdownItHighlightjs, { inline: true }) .render('console.log(42){.">js}'); console.log(reuslt_xss);	6.5	More Details
CVE-2020-7032	An XML external entity (XXE) vulnerability in Avaya WebLM admin interface allows authenticated users to read arbitrary files or conduct server-side request forgery (SSRF) attacks via a crafted DTD in an XML request. Affected versions of Avaya WebLM include: 7.0 through 7.1.3.6 and 8.0 through 8.1.2.	6.5	More Details
CVE-2020-26129	In JetBrains Ktor before 1.4.1, HTTP request smuggling was possible.	6.5	More Details
CVE-2020-8582	Element Software versions prior to 12.2 and HCI versions prior to 1.8P1 are susceptible to a vulnerability which could allow an authenticated user to view sensitive information.	6.5	More Details
CVE-2020-25988	UPNP Service listening on port 5555 in Genexis Platinum 4410 Router V2.1 (P4410-V2–1.34H) has an action 'X_GetAccess' which leaks the credentials of 'admin', provided that the attacker is network adjacent.	6.5	More Details
CVE-2020-13351	Insufficient permission checks in scheduled pipeline API in GitLab CE/EE 13.0+ allows an attacker to read variable names and values for scheduled pipelines on projects visible to the attacker. Affected versions are >=13.0, <13.3.9,>=13.4.0, <13.4.5,>=13.5.0, <13.5.2.	6.5	More Details
CVE-2020-27558	Use of an undocumented user in BASETech GE-131 BT-1837836 firmware 20180921 allows remote attackers to view the video stream.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4475	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5 and 6.0.0.0 through 6.0.3.2 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.	6.5	More Details
CVE-2020-4671	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.2 and 5.2.0.0 through 5.2.6.5 stores potentially sensitive information in log files that could be read by an authenticatedl user. IBM X-Force ID: 186284.	6.5	More Details
CVE-2020-4692	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.2 and 5.2.0.0 through 5.2.6.5 could allow an authenticated user to obtain sensitive information from the Dashboard UI. IBM X-Force ID: 186780.	6.5	More Details
CVE-2020-4566	IBM Sterling B2B Integrator Standard Edition 5.2.6.0 through 5.2.6.5 and 6.0.0.0 through 6.0.3.2 stores potentially highly sensitive information in log files that could be read by an authenticated user. IBM X-Force ID: 184083.	6.5	More Details
CVE-2020-8746	Integer overflow in subsystem for Intel(R) AMT versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70 and 14.0.45 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2020-7770	This affects the package json8 before 1.0.3. The function adds in the target object the property specified in the path, however it does not properly check the key being set, leading to a prototype pollution.	6.5	More Details
CVE-2020-12349	Improper input validation in the Intel(R) Data Center Manager Console before version 3.6.2 may allow an authenticated user to potentially enable information disclosure via network access.	6.5	More Details
CVE-2020-17040	Windows Hyper-V Security Feature Bypass Vulnerability	6.5	More Details
CVE-2020-12322	Improper input validation in some Intel(R) Wireless Bluetooth(R) products before version 21.110 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2020-12319	Insufficient control flow management in some Intel(R) PROSet/Wireless WiFi products before version 21.110 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2020-12317	Improper buffer restriction in some Intel(R) PROSet/Wireless WiFi products before version 21.110 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12314	Improper input validation in some Intel(R) PROSet/Wireless WiFi products before version 21.110 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2020-8766	Improper conditions check in the Intel(R) SGX DCAP software before version 1.6 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2020-8669	Improper input validation in the Intel(R) Data Center Manager Console before version 3.6.2 may allow an authenticated user to potentially enable information disclosure via network access.	6.5	More Details
CVE-2020-12308	Improper access control for the Intel(R) Computing Improvement Program before version 2.4.5982 may allow an unprivileged user to potentially enable information disclosure via network access.	6.5	More Details
CVE-2020-12353	Improper permissions in the Intel(R) Data Center Manager Console before version 3.6.2 may allow an authenticated user to potentially enable denial of service via network access.	6.5	More Details
CVE-2020-8755	Race condition in subsystem for Intel(R) CSME versions before 12.0.70 and 14.0.45, Intel(R) SPS versions before E5_04.01.04.400 and E3_05.01.04.200 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.4	More Details
CVE-2020-28650	The WPBakery plugin before 6.4.1 for WordPress allows XSS because it calls kses_remove_filters to disable the standard WordPress XSS protection mechanism for the Author and Contributor roles.	6.4	More Details
CVE-2020-8354	A potential vulnerability in the SMI callback function used in the VariableServiceSmm driver in some Lenovo Notebook models may allow arbitrary code execution.	6.4	More Details
CVE-2020-12926	The Trusted Platform Modules (TPM) reference software may not properly track the number of times a failed shutdown happens. This can leave the TPM in a state where confidential key material in the TPM may be able to be compromised. AMD believes that the attack requires physical access of the device because the power must be repeatedly turned on and off. This potential attack may be used to change confidential information, alter executables signed by key material in the TPM, or create a denial of service of the device.	6.4	More Details
CVE-2020-7033	A Cross Site Scripting (XSS) Vulnerability on the Unified Portal Client (web client) used in Avaya Equinox Conferencing can allow an authenticated user to perform XSS attacks. The affected versions of Equinox Conferencing includes all 9.x versions before 9.1.10.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16985	Azure Sphere Information Disclosure Vulnerability	6.2	More Details
CVE-2020-0584	Buffer overflow in firmware for Intel(R) SSD DC P4800X and P4801X Series, Intel(R) Optane(TM) SSD 900P and 905P Series may allow an unauthenticated user to potentially enable a denial of service via local access.	6.2	More Details
CVE-2020-17085	Microsoft Exchange Server Denial of Service Vulnerability	6.2	More Details
CVE-2020-16990	Azure Sphere Information Disclosure Vulnerability	6.2	More Details
CVE-2020-16986	Azure Sphere Denial of Service Vulnerability	6.2	More Details
CVE-2020-13954	By default, Apache CXF creates a /services page containing a listing of the available endpoint names and addresses. This webpage is vulnerable to a reflected Cross-Site Scripting (XSS) attack via the styleSheetPath, which allows a malicious actor to inject javascript into the web page. This vulnerability affects all versions of Apache CXF prior to 3.4.1 and 3.3.8. Please note that this is a separate issue to CVE-2019-17573.	6.1	More Details
CVE-2020-24442	Adobe Connect version 11.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	6.1	More Details
CVE-2020-24443	Adobe Connect version 11.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	6.1	More Details
CVE-2020-27459	Chronoforeum 2.0.11 allows Stored XSS vulnerabilities when inserting a crafted payload into a post. If any user sees the post, the inserted XSS code is executed.	6.1	More Details
CVE-2020-27627	JetBrains TeamCity before 2020.1.2 was vulnerable to URL injection.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28139	SourceCodester Online Clothing Store 1.0 is affected by a cross-site scripting (XSS) vulnerability via a Offer Detail field in offer.php.	6.1	More Details
CVE-2020-11860	Cross-Site Scripting vulnerability on Micro Focus ArcSight Logger product, affecting all version prior to 7.1.1. The vulnerability could be remotely exploited resulting in Cross-Site Scripting (XSS)	6.1	More Details
CVE-2020-25890	The web application of Kyocera printer (ECOSYS M2640IDW) is affected by Stored XSS vulnerability, discovered in the addition a new contact in "Machine Address Book". Successful exploitation of this vulnerability can lead to session hijacking of the administrator in the web application or the execution of unwanted actions	6.1	More Details
CVE-2020-28415	A reflected cross-site scripting (XSS) vulnerability exists in the TranzWare Payment Gateway 3.1.12.3.2. A remote unauthenticated attacker is able to execute arbitrary HTML code via crafted url (different vector than CVE-2020-28414).	6.1	More Details
CVE-2020-27193	A cross-site scripting (XSS) vulnerability in the Color Dialog plugin for CKEditor 4.15.0 allows remote attackers to run arbitrary web script after persuading a user to copy and paste crafted HTML code into one of editor inputs.	6.1	More Details
CVE-2020-28129	Stored Cross-site scripting (XSS) vulnerability in SourceCodester Gym Management System 1.0 allows users to inject and store arbitrary JavaScript code in index.php?page=packages via vulnerable fields 'Package Name' and 'Description'.	6.1	More Details
CVE-2020-28092	PESCMS Team 2.3.2 has multiple reflected XSS via the id parameter:? g=Team&m=Task&a=my&status=3&id=,? g=Team&m=Task&a=my&status=0&id=,? g=Team&m=Task&a=my&status=1&id=,? g=Team&m=Task&a=my&status=10&id=	6.1	More Details
CVE-2020-16982	Azure Sphere Unsigned Code Execution Vulnerability	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26825	SAP Fiori Launchpad (News tile Application), versions - 750,751,752,753,754,755, allows an unauthorized attacker to use SAP Fiori Launchpad News tile Application to send malicious code, to a different end user (victim), because News tile does not sufficiently encode user controlled inputs, resulting in Reflected Cross-Site Scripting (XSS) vulnerability. Information maintained in the victim's web browser can be read, modified, and sent to the attacker. The malicious code cannot significantly impact the victim's browser and the victim can easily close the browser tab to terminate it.	6.1	More Details
CVE-2020-16981	Azure Sphere Elevation of Privilege Vulnerability	6.1	More Details
CVE-2020-28414	A reflected cross-site scripting (XSS) vulnerability exists in the TranzWare Payment Gateway 3.1.12.3.2. A remote unauthenticated attacker is able to execute arbitrary HTML code via crafted url (different vector than CVE-2020-28415).	6.1	More Details
CVE-2020-16983	Azure Sphere Tampering Vulnerability	5.7	More Details
CVE-2020-13348	An issue has been discovered in GitLab EE affecting all versions starting from 10.2. Required CODEOWNERS approval could be bypassed by targeting a branch without the CODEOWNERS file. Affected versions are >=10.2, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.	5.7	More Details
CVE-2020-7765	This affects the package @firebase/util before 0.3.4. This vulnerability relates to the deepExtend function within the DeepCopy.ts file. Depending on if user input is provided, an attacker can overwrite and pollute the object prototype of a program.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11123	u'information disclosure in gatekeeper trustzone implementation as the throttling mechanism to prevent brute force attempts at getting user`s lock-screen password can be bypassed by performing the standard gatekeeper operations.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8009W, APQ8017, APQ8037, APQ8053, APQ8064AU, APQ8096, APQ8096AU, APQ8096SG, APQ8098, MDM8207, MDM9150, MDM9205, MDM9206, MDM9207, MDM9250, MDM9607, MDM9628, MDM9640, MDM9650, MDM9655, MSM8108, MSM8208, MSM8209, MSM8608, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8996SG, MSM8998, QCM4290, QCS405, QCS410, QCS4290, QCS603, QCS605, QCS610, QM215, QSM8250, QSM8350, SA415M, SA515M, SA6145P, SA6150P, SA6155, SA6155P, SA8150P, SA8155, SA8155P, SA8195P, SC7180, SC8180X, SC8180XP, SDA429W, SDA640, SDA660, SDA670, SDA845, SDA855, SDM1000, SDM429, SDM429W, SDM439, SDM450, SDM455, SDM630, SDM632, SDM636, SDM640, SDM660, SDM670, SDM710, SDM712, SDM830, SDM845, SDM850, SDW2500, SDX24, SDX50M, SDX55, SDX55M, SM4125, SM4250, SM4250P, SM6115, SM6115P, SM6125, SM6150, SM6150P, SM6250, SM6250P, SM6350, SM7125, SM7150, SM7150P, SM7225, SM7250, SM7250P, SM8150, SM8150P, SM8250, SM8350, SM8350P, SXR1120, SXR1130, SXR2130, SXR2130P, WCD9330	5.5	More Details
CVE-2020-17046	Windows Error Reporting Denial of Service Vulnerability	5.5	More Details
CVE-2020-17083	Microsoft Exchange Server Remote Code Execution Vulnerability	5.5	More Details
CVE-2020-17045	Windows KernelStream Information Disclosure Vulnerability	5.5	More Details
CVE-2020-11209	Improper authorization in DSP process could allow unauthorized users to downgrade the library versions in SD820, SD821, SD820, QCS603, QCS605, SDA855, SA6155P, SA6145P, SA6155, SA6155P, SD855, SD 675, SD660, SD429, SD439	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17036	Windows Function Discovery SSDP Provider Information Disclosure Vulnerability	5.5	More Details
CVE-2020-24460	Incorrect default permissions in the Intel(R) DSA before version 20.8.30.6 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-12912	A potential vulnerability in the AMD extension to Linux "hwmon" service may allow an attacker to use the Linux-based Running Average Power Limit (RAPL) interface to show various side channel attacks. In line with industry partners, AMD has updated the RAPL interface to require privileged access.	5.5	More Details
CVE-2020-17030	Windows MSCTF Server Information Disclosure Vulnerability	5.5	More Details
CVE-2020-17013	Win32k Information Disclosure Vulnerability	5.5	More Details
CVE-2020-17056	Windows Network File System Information Disclosure Vulnerability	5.5	More Details
CVE-2020-17029	Windows Canonical Display Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2020-17069	Windows NDIS Information Disclosure Vulnerability	5.5	More Details
CVE-2020-17071	Windows Delivery Optimization Information Disclosure Vulnerability	5.5	More Details
CVE-2020-1599	Windows Spoofing Vulnerability	5.5	More Details
CVE-2020-17081	Microsoft Raw Image Extension Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17113	Windows Camera Codec Information Disclosure Vulnerability	5.5	More Details
CVE-2020-17102	WebP Image Extensions Information Disclosure Vulnerability	5.5	More Details
CVE-2020-8694	Insufficient access control in the Linux kernel driver for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-8695	Observable discrepancy in the RAPL interface for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-8696	Improper removal of sensitive information before storage or transfer in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-8698	Improper isolation of shared resources in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-17100	Visual Studio Tampering Vulnerability	5.5	More Details
CVE-2020-16999	Windows WalletService Information Disclosure Vulnerability	5.5	More Details
CVE-2020-17000	Remote Desktop Protocol Client Information Disclosure Vulnerability	5.5	More Details
CVE-2020-24441	Adobe Acrobat Reader for Android version 20.6.2 (and earlier) does not properly restrict access to directories created by the application. This could result in disclosure of sensitive information stored in databases used by the application. Exploitation requires a victim to download and run a malicious application.	5.5	More Details
CVE-2020-17004	Windows Graphics Component Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8767	Uncaught exception in the Intel(R) 50GbE IP Core for Intel(R) Quartus Prime before version 20.2 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-27557	Unprotected Storage of Credentials vulnerability in BASETech GE-131 BT-1837836 firmware 20180921 allows local users to gain access to the video streaming username and password via SQLite files containing plain text credentials.	5.5	More Details
CVE-2020-0573	Out of bounds read in the Intel CSI2 Host Controller driver may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-0575	Improper buffer restrictions in the Intel(R) Unite Client for Windows* before version 4.2.13064 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-12316	Insufficiently protected credentials in the Intel(R) EMA before version 1.3.3 may allow an authorized user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-12326	Improper initialization in some Intel(R) Thunderbolt(TM) DCH drivers for Windows* before version 72 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-27990	Nagios XI before 5.7.5 is vulnerable to XSS in the Deployment tool (add agent).	5.4	More Details
CVE-2020-27991	Nagios XI before 5.7.5 is vulnerable to XSS in Account Information (Email field).	5.4	More Details
CVE-2020-28647	In Progress MOVEit Transfer before 2020.1, a malicious user could craft and store a payload within the application. If a victim within the MOVEit Transfer instance interacts with the stored payload, it could invoke and execute arbitrary code within the context of the victim's browser (XSS).	5.4	More Details
CVE-2020-27989	Nagios XI before 5.7.5 is vulnerable to XSS in Dashboard Tools (Edit Dashboard).	5.4	More Details
CVE-2020-27988	Nagios XI before 5.7.5 is vulnerable to XSS in Manage Users (Username field).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17018	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2020-4672	IBM Business Automation Workflow 20.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186285.	5.4	More Details
CVE-2020-1325	Azure DevOps Server and Team Foundation Services Spoofing Vulnerability	5.4	More Details
CVE-2020-17021	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2020-13773	Ivanti Endpoint Manager through 2020.1.1 allows XSS via /LDMS/frm_splitfrm.aspx, /LDMS/licensecheck.aspx, /LDMS/frm_splitcollapse.aspx, /LDMS/alert_log.aspx, /LDMS/ServerList.aspx, /LDMS/frm_coremainfrm.aspx, /LDMS/frm_findfrm.aspx, /LDMS/frm_taskfrm.aspx, and /LDMS/query_browsecomp.aspx.	5.4	More Details
CVE-2020-17060	Microsoft SharePoint Server Spoofing Vulnerability	5.4	More Details
CVE-2020-25798	A stored cross-site scripting (XSS) vulnerability in LimeSurvey before and including 3.21.1 allows authenticated users with correct permissions to inject arbitrary web script or HTML via parameter ParticipantAttributeNamesDropdown of the Attributes on the central participant database page. When the survey attribute being edited or viewed, e.g. by an administrative user, the JavaScript code will be executed in the browser.	5.4	More Details
CVE-2020-25832	Reflected Cross Site scripting vulnerability on Micro Focus Filr product, affecting version 4.2.1. The vulnerability could be exploited to perform Reflected XSS attack.	5.4	More Details
CVE-2020-17006	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5663	Stored cross-site scripting vulnerability in XooNIps 3.49 and earlier allows remote authenticated attackers to inject arbitrary script via unspecified vectors.	5.4	More Details
CVE-2020-5662	Reflected cross-site scripting vulnerability in XooNIps 3.49 and earlier allows remote authenticated attackers to inject arbitrary script via unspecified vectors.	5.4	More Details
CVE-2020-25834	Cross-Site Scripting vulnerability on Micro Focus ArcSight Logger product, affecting version 7.1. The vulnerability could be remotely exploited resulting in Cross-Site Scripting (XSS).	5.4	More Details
CVE-2020-25706	A cross-site scripting (XSS) vulnerability exists in templates_import.php (Cacti 1.2.13) due to Improper escaping of error message during template import preview in the xml_path field	5.4	More Details
CVE-2020-17005	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2020-26701	Cross-site scripting (XSS) vulnerability in Dashboards section in Kaa IoT Platform v1.2.0 allows remote attackers to inject malicious web scripts or HTML Injection payloads via the Description parameter.	5.4	More Details
CVE-2020-16993	Azure Sphere Elevation of Privilege Vulnerability	5.4	More Details
CVE-2020-16989	Azure Sphere Elevation of Privilege Vulnerability	5.4	More Details
CVE-2020-26406	Certain SAST CiConfiguration information could be viewed by unauthorized users in GitLab EE starting with 13.3. This information was exposed through GraphQL to non-members of public projects with repository visibility restricted as well as guest members on private projects. Affected versions are: >=13.3, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.	5.3	More Details
CVE-2020-28247	The lettre library through 0.10.0-alpha for Rust allows arbitrary sendmail option injection via transport/sendmail/mod.rs.	5.3	More Details
CVE-2020-27629	In JetBrains TeamCity before 2020.1.5, secure dependency parameters could be not masked in depending builds when there are no internal artifacts.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27626	JetBrains YouTrack before 2020.3.5333 was vulnerable to SSRF.	5.3	More Details
CVE-2020-7767	All versions of package express-validators are vulnerable to Regular Expression Denial of Service (ReDoS) when validating specifically-crafted invalid urls.	5.3	More Details
CVE-2020-27622	In JetBrains IntelliJ IDEA before 2020.2, the built-in web server could expose information about the IDE version.	5.3	More Details
CVE-2020-17494	Untangle Firewall NG before 16.0 uses MD5 for passwords.	5.3	More Details
CVE-2020-17017	Microsoft SharePoint Information Disclosure Vulnerability	5.3	More Details
CVE-2020-1999	A vulnerability exists in the Palo Alto Network PAN-OS signature-based threat detection engine that allows an attacker to communicate with devices in the network in a way that is not analyzed for threats by sending data through specifically crafted TCP packets. This technique evades signature-based threat detection. This issue impacts: PAN-OS 8.1 versions earlier than 8.1.17; PAN-OS 9.0 versions earlier than 9.0.11; PAN-OS 9.1 versions earlier than 9.1.5; All versions of PAN-OS 7.1 and PAN-OS 8.0.	5.3	More Details
CVE-2020-13772	In /ldclient/ldprov.cgi in Ivanti Endpoint Manager through 2020.1.1, an attacker is able to disclose information about the server operating system, local pathnames, and environment variables with no authentication required.	5.3	More Details
CVE-2020-7962	An issue was discovered in One Identity Password Manager 5.8. An attacker could enumerate valid answers for a user. It is possible for an attacker to detect a valid answer based on the HTTP response content, and reuse this answer later for a password reset on a chosen password. The enumeration is possible because, within the HTTP response content, WRONG ID is only returned when the answer is incorrect.	5.3	More Details
CVE-2020-17090	Microsoft Defender for Endpoint Security Feature Bypass Vulnerability	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27625	In JetBrains YouTrack before 2020.3.888, notifications might have mentioned inaccessible issues.	5.3	More Details
CVE-2020-27624	JetBrains YouTrack before 2020.3.888 was vulnerable to SSRF.	5.3	More Details
CVE-2020-27556	A predictable device ID in BASETech GE-131 BT-1837836 firmware 20180921 allows unauthenticated remote attackers to connect to the device.	5.3	More Details
CVE-2020-25210	In JetBrains YouTrack before 2020.3.7955, an attacker could access workflow rules without appropriate access grants.	5.3	More Details
CVE-2020-16979	Microsoft SharePoint Information Disclosure Vulnerability	5.3	More Details
CVE-2020-7333	Cross site scripting vulnerability in the firewall ePO extension of McAfee Endpoint Security (ENS) prior to 10.7.0 November 2020 Update allows administrators to inject arbitrary web script or HTML via the configuration wizard.	4.8	More Details
CVE-2020-4705	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.2 and 5.2.0.0 through 5.2.6.5 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: 187190.	4.8	More Details
CVE-2020-8897	A weak robustness vulnerability exists in the AWS Encryption SDKs for Java, Python, C and Javalcript prior to versions 2.0.0. Due to the non-committing property of AES-GCM (and other AEAD ciphers such as AES-GCM-SIV or (X)ChaCha20Poly1305) used by the SDKs to encrypt messages, an attacker can craft a unique cyphertext which will decrypt to multiple different results, and becomes especially relevant in a multi-recipient setting. We recommend users update their SDK to 2.0.0 or later.	4.8	More Details
CVE-2020-25833	Persistent cross-Site Scripting vulnerability on Micro Focus IDOL product, affecting all version prior to version 12.7. The vulnerability could be exploited to perform Persistent XSS attack.	4.8	More Details
CVE-2020-10776	A flaw was found in Keycloak before version 12.0.0, where it is possible to add unsafe schemes for the redirect_uri parameter. This flaw allows an attacker to perform a Cross-site scripting attack.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26219	touchbase.ai before version 2.0 is vulnerable to Open Redirect. Impacts can be many, and vary from theft of information and credentials, to the redirection to malicious websites containing attacker-controlled content, which in some cases even cause XSS attacks. So even though an open redirection might sound harmless at first, the impacts of it can be severe should it be exploitable. The issue is fixed in version 2.0.	4.7	More Details
CVE-2020-13358	A vulnerability in the internal Kubernetes agent api in GitLab CE/EE version 13.3 and above allows unauthorized access to private projects. Affected versions are: >=13.4, <13.4.5,>=13.3, <13.3.9,>=13.5, <13.5.2.	4.7	More Details
CVE-2020-12309	Insufficiently protected credentialsin subsystem in some Intel(R) Client SSDs and some Intel(R) Data Center SSDs may allow an unauthenticated user to potentially enable information disclosure via physical access.	4.6	More Details
CVE-2020-8761	Inadequate encryption strength in subsystem for Intel(R) CSME versions before 13.0.40 and 13.30.10 may allow an unauthenticated user to potentially enable information disclosure via physical access.	4.6	More Details
CVE-2020-8751	Insufficient control flow management in subsystem for Intel(R) CSME versions before 11.8.80, Intel(R) TXE versions before 3.1.80 may allow an unauthenticated user to potentially enable information disclosure via physical access.	4.6	More Details
CVE-2019-19556	An authentication bypass in the debug interface in Mercedes-Benz HERMES 1 allows an attacker with physical access to device hardware to obtain system information.	4.6	More Details
CVE-2019-19560	An authentication bypass in the debug interface in Mercedes-Benz HERMES 1.5 allows an attacker with physical access to device hardware to obtain system information.	4.6	More Details
CVE-2019-19562	An authentication bypass in the debug interface in Mercedes-Benz HERMES 2.1 allows an attacker with physical access to device hardware to obtain system information.	4.6	More Details
CVE-2020-12311	Insufficient control flow managementin firmware in some Intel(R) Client SSDs and some Intel(R) Data Center SSDs may allow an unauthenticated user to potentially enable information disclosure via physical access.	4.6	More Details
CVE-2020-12310	Insufficient control flow managementin firmware in some Intel(R) Client SSDs and some Intel(R) Data Center SSDs may allow an unauthenticated user to potentially enable information disclosure via physical access.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25746	QED ResourceXpress Qubi3 devices before 1.40.9 could allow a local attacker (with physical access to the device) to obtain sensitive information via the debug interface (keystrokes over a USB cable), aka wireless password visibility.	4.6	More Details
CVE-2020-8152	Insufficient protection of the server-side encryption keys in Nextcloud Server 19.0.1 allowed an attacker to replace the public key to decrypt them later on.	4.4	More Details
CVE-2020-12356	Out-of-bounds read in subsystem in Intel(R) AMT versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70 and 14.0.45 may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2020-12328	Protection mechanism failure in some Intel(R) Thunderbolt(TM) DCH drivers for Windows* before version 72 may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2020-8677	Improper access control in the Intel(R) Visual Compute Accelerator 2, all versions, may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-12327	Insecure default variable initialization in some Intel(R) Thunderbolt(TM) DCH drivers for Windows* before version 72 may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2020-9128	FusionCompute versions 8.0.0 have an insecure encryption algorithm vulnerability. Attackers with high permissions can exploit this vulnerability to cause information leak.	4.4	More Details
CVE-2020-13354	A potential DOS vulnerability was discovered in GitLab CE/EE starting with version 12.6. The container registry name check could cause exponential number of backtracks for certain user supplied values resulting in high CPU usage. Affected versions are: >=12.6, <13.3.9.	4.3	More Details
CVE-2020-13349	An issue has been discovered in GitLab EE affecting all versions starting from 8.12. A regular expression related to a file path resulted in the Advanced Search feature susceptible to catastrophic backtracking. Affected versions are >=8.12, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.	4.3	More Details
CVE-2020-6157	Opera Touch for iOS before version 2.4.5 is vulnerable to an address bar spoofing attack. The vulnerability allows a malicious page to trick the browser into showing an address of a different page. This may allow the malicious page to impersonate another page and trick a user into providing sensitive data.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4763	IBM Sterling File Gateway 6.0.0.0 through 6.0.3.2 and 2.2.0.0 through 2.2.6.5 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: 188897.	4.3	More Details
CVE-2020-4665	IBM Sterling File Gateway 2.2.0.0 through 2.2.6.5 and 6.0.0.0 through 6.0.3.2 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: 186280.	4.3	More Details
CVE-2020-27628	In JetBrains TeamCity before 2020.1.5, the Guest user had access to audit records.	4.3	More Details
CVE-2020-17015	Microsoft SharePoint Server Spoofing Vulnerability	4.3	More Details
CVE-2020-17048	Chakra Scripting Engine Memory Corruption Vulnerability	4.2	More Details
CVE-2020-17054	Chakra Scripting Engine Memory Corruption Vulnerability	4.2	More Details
CVE-2020-13352	Private group info is leaked leaked in GitLab CE/EE version 10.2 and above, when the project is moved from private to public group. Affected versions are: >=10.2, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.	3.7	More Details
CVE-2020-26220	toucbase.ai before version 2.0 leaks information by not stripping exif data from images. Anyone with access to the uploaded image of other users could obtain its geolocation, device, and software version data etc (if present. The issue is fixed in version 2.0.	3.5	More Details
CVE-2020-4886	IBM InfoSphere Information Server 11.7 stores sensitive information in the browser's history that could be obtained by a user who has access to the same system. IBM X-Force ID: 190910.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16126	An Ubuntu-specific modification to AccountsService in versions before 0.6.55-0ubuntu13.2, among other earlier versions, improperly dropped the ruid, allowing untrusted users to send signals to AccountService, thus stopping it from handling D-Bus messages in a timely fashion.	3.3	More Details
CVE-2020-17020	Microsoft Word Security Feature Bypass Vulnerability	3.3	More Details
CVE-2020-24366	Sensitive information could be disclosed in the JetBrains YouTrack application before 2020.2.0 for Android via application backups.	3.3	More Details
CVE-2020-2048	An information exposure through log file vulnerability exists where the password for the configured system proxy server for a PAN-OS appliance may be displayed in cleartext when using the CLI in Palo Alto Networks PAN-OS software. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.17; PAN-OS 9.0 versions earlier than PAN-OS 9.0.11; PAN-OS 9.1 versions earlier than PAN-OS 9.1.2.	3.3	More Details
CVE-2020-13350	CSRF in runner administration page in all versions of GitLab CE/EE allows an attacker who's able to target GitLab instance administrators to pause/resume runners. Affected versions are >=13.5.0, <13.5.2,>=13.4.0, <13.4.5,<13.3.9.	3.1	More Details
CVE-2020-16127	An Ubuntu-specific modification to AccountsService in versions before 0.6.55-0ubuntu13.2, among other earlier versions, would perform unbounded read operations on user-controlled ~/.pam_environment files, allowing an infinite loop if /dev/zero is symlinked to this location.	2.8	More Details
CVE-2020-13353	When importing repos via URL, one time use git credentials were persisted beyond the expected time window in Gitaly 1.79.0 or above.	2.5	More Details
CVE-2019-19557	A misconfiguration in the debug interface in Mercedes-Benz HERMES 1 allows an attacker with direct physical access to device hardware to obtain cellular modem information.	2.4	More Details
CVE-2019-19563	A misconfiguration in the debug interface in Mercedes-Benz HERMES 2.1 allows an attacker with direct physical access to device hardware to obtain cellular modem information.	2.4	More Details
CVE-2020-8352	In some Lenovo Desktop models, the Configuration Change Detection BIOS setting failed to detect SATA configuration changes.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19561	A misconfiguration in the debug interface in Mercedes-Benz HERMES 1.5 allows an attacker with direct physical access to device hardware to obtain cellular modem information.	2.4	More Details
CVE-2020-5424	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-2020-16091	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-27708. Reason: This candidate is a reservation duplicate of [ID]. Notes: All CVE users should reference CVE-2020-27708 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details