SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 13 January 2021

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-2021-21465	The BW Database Interface allows an attacker with low privileges to execute any crafted database queries, exposing the backend database. An attacker can include their own SQL commands which the database will execute without properly sanitizing the untrusted data leading to SQL injection vulnerability which can fully compromise the affected SAP system.	9.9	More Details
CVE-2020-26085	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory.	9.9	More Details
CVE-2020-8584	Element OS versions prior to 1.8P1 and 12.2 are susceptible to a vulnerability that could allow an unauthenticated remote attacker to perform arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11995	A deserialization vulnerability existed in dubbo 2.7.5 and its earlier versions, which could lead to malicious code execution. Most Dubbo users use Hessian2 as the default serialization/deserialization protool, during Hessian2 deserializing the HashMap object, some functions in the classes stored in HasMap will be executed after a series of program calls, however, those special functions may cause remote command execution. For example, the hashCode() function of the EqualsBean class in rome-1.7.0.jar will cause the remotely load malicious classes and execute malicious code by constructing a malicious request. This issue was fixed in Apache Dubbo 2.6.9 and 2.7.8.	9.8	More Details
CVE-2020-13451	An incomplete-cleanup vulnerability in the Office rendering engine of Gotenberg through 6.2.1 allows an attacker to overwrite LibreOffice configuration files and execute arbitrary code via macros.	9.8	More Details
CVE-2020-13452	In Gotenberg through 6.2.1, insecure permissions for tini (writable by user gotenberg) potentially allow an attacker to overwrite the file, which can lead to denial of service or code execution.	9.8	More Details
CVE-2020-7784	This affects all versions of package ts-process-promises. The injection point is located in line 45 in main entry of package in lib/process-promises.js. The vulnerability is demonstrated with the following PoC:	9.8	More Details
CVE-2020-7794	This affects all versions of package buns. The injection point is located in line 678 in index file lib/index.js in the exported function install(requestedModule).	9.8	More Details
CVE-2020-35131	Cockpit before 0.6.1 allows an attacker to inject custom PHP code and achieve Remote Command Execution via registerCriteriaFunction in lib/MongoLite/Database.php, as demonstrated by values in JSON data to the /auth/check or /auth/requestreset URI.	9.8	More Details
CVE-2020-35205	Server Side Request Forgery (SSRF) in Web Compliance Manager in Quest Policy Authority version 8.1.2.200 allows attackers to scan internal ports and make outbound connections via the initFile.jsp file. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details
CVE-2021-3118	EVOLUCARE ECSIMAGING (aka ECS Imaging) through 6.21.5 has multiple SQL Injection issues in the login form and the password-forgotten form (such as /req_password_user.php?email=). This allows an attacker to steal data in the database and obtain access to the application. (The database component runs as root.) NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details
CVE-2020-24027	In Live Networks, Inc., liblivemedia version 20200625, there is a potential buffer overflow bug in the server handling of a RTSP "PLAY" command, when the command specifies seeking by absolute time.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17500	Barco TransForm NDN-210 Lite, NDN-210 Pro, NDN-211 Lite, and NDN-211 Pro before 3.8 allows Command Injection (issue 1 of 4). The NDN-210 has a web administration panel which is made available over https. The logon method is basic authentication. There is a command injection issue that will result in unauthenticated remote code execution in the username and password fields of the logon prompt. The NDN-210 is part of Barco TransForm N solution and includes the patch from TransForm N version 3.8 onwards.	9.8	More Details
CVE-2020-0471	In reassemble_and_dispatch of packet_fragmenter.cc, there is a possible way to inject packets into an encrypted Bluetooth connection due to improper input validation. This could lead to remote escalation of privilege between two Bluetooth devices by a proximal attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-8.0, Android-8.1, Android-9, Android-10, Android-11; Android ID: A-169327567.	9.8	More Details
CVE-2021-0316	In avrc_pars_vendor_cmd of avrc_pars_tg.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11, Android-8.0, Android-8.1, Android-9, Android-10; Android ID: A-168802990.	9.8	More Details
CVE-2020-27637	The R programming language's default package manager CRAN is affected by a path traversal vulnerability that can lead to server compromise. This vulnerability affects packages installed via the R CMD install cli command or the install.packages() function from the interpreter. Update to version 4.0.3	9.8	More Details
CVE-2020-14275	Security vulnerability in HCL Commerce 9.0.0.5 through 9.0.0.13, 9.0.1.0 through 9.0.1.14 and 9.1 through 9.1.4 could allow denial of service, disclosure of user personal data, and performing of unauthorized administrative operations.	9.8	More Details
CVE-2020-26712	REDCap 10.3.4 contains a SQL injection vulnerability in the ToDoList function via sort parameter. The application uses the addition of a string of information from the submitted user that is not validated well in the database query, resulting in an SQL injection vulnerability where an attacker can exploit and compromise all databases.	9.8	More Details
CVE-2020-35458	An issue was discovered in ClusterLabs Hawk 2.x through 2.3.0-x. There is a Ruby shell code injection issue via the hawk_remember_me_id parameter in the login_from_cookie cookie. The user logout routine could be used by unauthenticated remote attackers to execute code as hauser.	9.8	More Details
CVE-2021-3129	Ignition before 2.5.2, as used in Laravel and other products, allows unauthenticated remote attackers to execute arbitrary code because of insecure usage of file_get_contents() and file_put_contents(). This is exploitable on sites using debug mode with Laravel before 8.4.2.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15800	A vulnerability has been identified in SCALANCE X-200 switch family (incl. SIPLUS NET variants) (All versions < V5.2.5), SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) (All versions < V5.5.0), SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants) (All versions < V4.1.0). The webserver of the affected devices contains a vulnerability that may lead to a heap overflow condition. An attacker could cause this condition on the webserver by sending specially crafted requests. This could stop the webserver temporarily.	9.8	More Details
CVE-2020-13450	A directory traversal vulnerability in file upload function of Gotenberg through 6.2.1 allows an attacker to upload and overwrite any writable files outside the intended folder. This can lead to DoS, a change to program behavior, or code execution.	9.8	More Details
CVE-2020-25226	A vulnerability has been identified in SCALANCE X-200 switch family (incl. SIPLUS NET variants) (All versions < V5.2.5), SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) (All versions < V5.5.0). The web server of the affected devices contains a vulnerability that may lead to a buffer overflow condition. An attacker could cause this condition on the webserver by sending a specially crafted request. The webserver could stop and not recover anymore.	9.8	More Details
CVE-2019-18643	Rock RMS versions before 8.10 and versions 9.0 through 9.3 fails to properly validate files uploaded in the application. The only protection mechanism is a file-extension blacklist that can be bypassed by adding multiple spaces and periods after the file name. This could allow an attacker to upload ASPX code and gain remote code execution on the application. The application typically runs as LocalSystem as mandated in the installation guide. Patched in versions 8.10 and 9.4.	9.8	More Details
CVE-2021-3029	EVOLUCARE ECSIMAGING (aka ECS Imaging) through 6.21.5 has an OS Command Injection vulnerability via shell metacharacters and an IFS manipulation. The parameter "file" on the webpage /showfile.php can be exploited to gain root access. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details
CVE-2020-26972	The lifecycle of IPC Actors allows managed actors to outlive their manager actors; and the former must ensure that they are not attempting to use a dead actor they have a reference to. Such a check was omitted in WebGL, resulting in a use-after-free and a potentially exploitable crash. This vulnerability affects Firefox < 84.	9.8	More Details
CVE-2020-36178	oal_ipt_addBridgeIsolationRules on TP-Link TL-WR840N 6_EU_0.9.1_4.16 devices allows OS command injection because a raw string entered from the web interface (an IP address field) is used directly for a call to the system library function (for iptables). NOTE: oal_ipt_addBridgeIsolationRules is not the only function that calls util_execSystem.	9.8	More Details
CVE-2020-26759	clickhouse-driver before 0.1.5 allows a malicious clickhouse server to trigger a crash or execute arbitrary code (on a database client) via a crafted server response, due to a buffer overflow.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36177	RsaPad_PSS in wolfcrypt/src/rsa.c in wolfSSL before 4.6.0 has an out-of-bounds write for certain relationships between key size and digest size.	9.8	More Details
CVE-2020-10655	The Proofpoint Insider Threat Management Server (formerly ObserveIT Server) before 7.9.1 contains a vulnerability in the ITM application server's WriteWindowMouse API. The vulnerability allows an anonymous remote attacker to execute arbitrary code with local administrator privileges. The vulnerability is caused by improper deserialization.	9.8	More Details
CVE-2020-10656	The Proofpoint Insider Threat Management Server (formerly ObserveIT Server) before 7.9.1 contains a vulnerability in the ITM application server's WriteWindowMouseWithChunksV2 API. The vulnerability allows an anonymous remote attacker to execute arbitrary code with local administrator privileges. The vulnerability is caused by improper deserialization.	9.8	More Details
CVE-2020-10658	The Proofpoint Insider Threat Management Server (formerly ObserveIT Server) before 7.9.1 contains a vulnerability in the ITM application server's WriteImage API. The vulnerability allows an anonymous remote attacker to execute arbitrary code with local administrator privileges. The vulnerability is caused by improper deserialization.	9.8	More Details
CVE-2012-10001	The Limit Login Attempts plugin before 1.7.1 for WordPress does not clear auth cookies upon a lockout, which might make it easier for remote attackers to conduct brute-force authentication attempts.	9.8	More Details
CVE-2019-18642	Rock RMS version before 8.6 is vulnerable to account takeover by tampering with the user ID parameter in the profile update feature. The lack of validation and use of sequential user IDs allows any user to change account details of any other user. This vulnerability could be used to change the email address of another account, even the administrator account. Upon changing another account's email address, performing a password reset to the new email address could allow an attacker to take over any account.	9.8	More Details
CVE-2021-21108	Use after free in media in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-21115	User after free in safe browsing in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-21111	Insufficient policy enforcement in WebUI in Google Chrome prior to 87.0.4280.141 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	9.6	More Details
CVE-2021-21109	Use after free in payments in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21110	Use after free in safe browsing in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-21107	Use after free in drag and drop in Google Chrome on Linux prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-16025	Heap buffer overflow in clipboard in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-16024	Heap buffer overflow in UI in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-16018	Use after free in payments in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-16017	Use after free in site isolation in Google Chrome prior to 86.0.4240.198 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-16016	Inappropriate implementation in base in Google Chrome prior to 86.0.4240.193 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-16014	Use after free in PPAPI in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-21106	Use after free in autofill in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-36166	An issue was discovered in Veritas InfoScale 7.x through 7.4.2 on Windows, Storage Foundation through 6.1 on Windows, Storage Foundation HA through 6.1 on Windows, and InfoScale Operations Manager (aka VIOM) Windows Management Server 7.x through 7.4.2. On start-up, it loads the OpenSSL library from \usr\local\ssl. This library attempts to load the \usr\local\ssl\openssl.cnf configuration file, which may not exist. On Windows systems, this path could translate to <drive>:\usr\local\ssl\openssl.cnf, where <drive> could be the default Windows installation drive such as C:\ or the drive where a Veritas product is installed. By default, on Windows systems, users can create directories under any top-level directory. A low privileged user can create a <drive>:\usr\local\ssl\openssl.cnf configuration file to load a malicious OpenSSL engine, resulting in arbitrary code execution as SYSTEM when the service starts. This gives the attacker administrator access on the system, allowing the attacker (by default) to access all data, access all installed applications, etc.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36163	An issue was discovered in Veritas NetBackup and OpsCenter through 8.3.0.1. NetBackup processes using Strawberry Perl attempt to load and execute libraries from paths that do not exist by default on the Windows operating system. By default, on Windows systems, users can create directories under C:\. If a low privileged user on the Windows system creates an affected path with a library that NetBackup attempts to load, they can execute arbitrary code as SYSTEM or Administrator. This gives the attacker administrator access on the system, allowing the attacker (by default) to access all data, access all installed applications, etc. This affects NetBackup master servers, media servers, clients, and OpsCenter servers on the Windows platform. The system is vulnerable during an install or upgrade on all systems and post-install on Master, Media, and OpsCenter servers during normal operations.	9.3	More Details
CVE-2020-36164	An issue was discovered in Veritas Enterprise Vault through 14.0. On start-up, it loads the OpenSSL library. The OpenSSL library then attempts to load the openssl.cnf configuration file (which does not exist) at the following locations in both the System drive (typically C:\) and the product's installation drive (typically not C:\): \Isode\etc\ssl\openssl.cnf (on SMTP Server) or \user\ssl\openssl.cnf (on other affected components). By default, on Windows systems, users can create directories under C:\. A low privileged user can create a openssl.cnf configuration file to load a malicious OpenSSL engine, resulting in arbitrary code execution as SYSTEM when the service starts. This gives the attacker administrator access on the system, allowing the attacker (by default) to access all data, access all installed applications, etc. This vulnerability only affects a server with MTP Server, SMTP Archiving IMAP Server, IMAP Archiving, Vault Cloud Adapter, NetApp File server, or File System Archiving for NetApp as File Server.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36165	An issue was discovered in Veritas Desktop and Laptop Option (DLO) before 9.4. On start-up, it loads the OpenSSL library from /ReleaseX64/ssl. This library attempts to load the /ReleaseX64/ssl/openssl.cnf configuration file, which does not exist. By default, on Windows systems, users can create directories under C:\. A low privileged user can create a C:/ReleaseX64/ssl/openssl.cnf configuration file to load a malicious OpenSSL engine, resulting in arbitrary code execution as SYSTEM when the service starts. This gives the attacker administrator access on the system, allowing the attacker (by default) to access all data, access all installed applications, etc. This impacts DLO server and client installations.	9.3	More Details
CVE-2020-36162	An issue was discovered in Veritas CloudPoint before 8.3.0.1+hotfix. The CloudPoint Windows Agent leverages OpenSSL. This OpenSSL library attempts to load the \usr\local\ssl\openssl.cnf configuration file, which does not exist. By default, on Windows systems users can create directories under <drive>:\. A low privileged user can create a <drive>:\usr\local\ssl\openssl.cnf configuration file to load a malicious OpenSSL engine, which may result in arbitrary code execution. This would give the attacker administrator access on the system, allowing the attacker (by default) to access all data, access all installed applications, etc.	9.3	More Details
CVE-2020-36167	An issue was discovered in the server in Veritas Backup Exec through 16.2, 20.6 before hotfix 298543, and 21.1 before hotfix 657517. On start-up, it loads the OpenSSL library from the Installation folder. This library in turn attempts to load the /usr/local/ssl/openssl.cnf configuration file, which may not exist. On Windows systems, this path could translate to <drive>:\usr\local\ssl\openssl.cnf. A low privileged user can create a :\usr\local\ssl\openssl.cnf configuration file to load a malicious OpenSSL engine, resulting in arbitrary code execution as SYSTEM when the service starts. This gives the attacker administrator access on the system, allowing the attacker (by default) to access all data, access all installed applications, etc. If the system is also an Active Directory domain controller, then this can affect the entire domain.	9.3	More Details
CVE-2020-36168	An issue was discovered in Veritas Resiliency Platform 3.4 and 3.5. It leverages OpenSSL on Windows systems when using the Managed Host addon. On start-up, it loads the OpenSSL library. This library may attempt to load the openssl.cnf configuration file, which does not exist. By default, on Windows systems, users can create directories under C:\. A low privileged user can create a C:\usr\local\ssl\openssl.cnf configuration file to load a malicious OpenSSL engine, resulting in arbitrary code execution as SYSTEM when the service starts. This gives the attacker administrator access on the system, allowing the attacker (by default) to access all data, access all installed applications, etc.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36169	An issue was discovered in Veritas NetBackup through 8.3.0.1 and OpsCenter through 8.3.0.1. Processes using OpenSSL attempt to load and execute libraries from paths that do not exist by default on the Windows operating system. By default, on Windows systems, users can create directories under the top level of any drive. If a low privileged user creates an affected path with a library that the Veritas product attempts to load, they can execute arbitrary code as SYSTEM or Administrator. This gives the attacker administrator access on the system, allowing the attacker (by default) to access all data, access all installed applications, etc. This vulnerability affects master servers, media servers, clients, and OpsCenter servers on the Windows platform. The system is vulnerable during an install or upgrade and post-install during normal operations.	9.3	More Details
CVE-2020-36160	An issue was discovered in Veritas System Recovery before 21.2. On start-up, it loads the OpenSSL library from \usr\local\ssl. This library attempts to load the from \usr\local\ssl\openssl.cnf configuration file, which does not exist. By default, on Windows systems, users can create directories under C:\. A low privileged user can create a C:\usr\local\ssl\openssl.cnf configuration file to load a malicious OpenSSL engine, resulting in arbitrary code execution as SYSTEM when the service starts. This gives the attacker administrator access on the system, allowing the attacker (by default) to access all data and installed applications, etc. If the system is also an Active Directory domain controller, then this can affect the entire domain.	9.3	More Details
CVE-2020-27285	The default configuration of Crimson 3.1 (Build versions prior to 3119.001) allows a user to be able to read and modify the database without authentication.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-36161	An issue was discovered in Veritas APTARE 10.4 before 10.4P9 and 10.5 before 10.5P3. By default, on Windows systems, users can create directories under C:\. A low privileged user can create a directory at the configuration file locations. When the Windows system restarts, a malicious OpenSSL engine could exploit arbitrary code execution as SYSTEM. This gives the attacker administrator access on the system, allowing the attacker (by default) to access all data, access all installed applications, etc.	8.8	More Details
CVE-2021-1678	Windows Print Spooler Spoofing Vulnerability	8.8	More Details
CVE-2021-21457	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21458	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21459	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21460	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated DIB file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21461	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated BMP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21462	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21463	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21466	SAP Business Warehouse, versions 700, 701, 702, 711, 730, 731, 740, 750, 782 and SAP BW/4HANA, versions 100, 200, allow a low privileged attacker to inject code using a remote enabled function module over the network. Via the function module an attacker can create a malicious ABAP report which could be used to get access to sensitive data, to inject malicious UPDATE statements that could have also impact on the operating system, to disrupt the functionality of the SAP system which can thereby lead to a Denial of Service.	8.8	More Details
CVE-2021-1636	Microsoft SQL Elevation of Privilege Vulnerability	8.8	More Details
CVE-2021-3025	Invision Community IPS Community Suite before 4.5.4.2 allows SQL Injection via the Downloads REST API (the sortDir parameter in a sortBy=popular action to the GETindex() method in applications/downloads/api/files.php).	8.8	More Details
CVE-2020-35745	PHPGURUKUL Hospital Management System V 4.0 does not properly restrict access to admin/dashboard.php, which allows attackers to access all data of users, doctors, patients, change admin password, get appointment history and access all session logs.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23630	A blind SQL injection vulnerability exists in zzcms ver201910 based on time (cookie injection).	8.8	More Details
CVE-2021-1658	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-1660	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-1664	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-1666	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-26773	Restaurant Reservation System 1.0 suffers from an authenticated SQL injection vulnerability, which allows a remote, authenticated attacker to execute arbitrary SQL commands via the date parameter in includes/reservation.inc.php.	8.8	More Details
CVE-2020-35114	Mozilla developers reported memory safety bugs present in Firefox 83. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 84.	8.8	More Details
CVE-2020-35113	Mozilla developers reported memory safety bugs present in Firefox 83 and Firefox ESR 78.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.	8.8	More Details
CVE-2020-35112	If a user downloaded a file lacking an extension on Windows, and then "Open"-ed it from the downloads panel, if there was an executable file in the downloads directory with the same name but with an executable extension (such as .bat or .exe) that executable would have been launched instead. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.	8.8	More Details
CVE-2021-1667	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-1669	Windows Remote Desktop Security Feature Bypass Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1671	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-1673	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-1674	Windows Remote Desktop Protocol Core Security Feature Bypass Vulnerability	8.8	More Details
CVE-2020-26974	When flex-basis was used on a table wrapper, a StyleGenericFlexBasis object could have been incorrectly cast to the wrong type. This resulted in a heap use-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.	8.8	More Details
CVE-2020-26973	Certain input to the CSS Sanitizer confused it, resulting in incorrect components being removed. This could have been used as a sanitizer bypass. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.	8.8	More Details
CVE-2021-21456	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated DIB file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21455	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated DIB file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21454	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated RLE file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2020-16029	Inappropriate implementation in PDFium in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to bypass navigation restrictions via a crafted PDF file.	8.8	More Details
CVE-2020-23960	Multiple cross-site request forgery (CSRF) vulnerabilities in the Admin Console in Fork before 5.8.3 allows remote attackers to perform unauthorized actions as administrator to (1) approve the mass of the user's comments, (2) restoring a deleted user, (3) installing or running modules, (4) resetting the analytics, (5) pinging the mailmotor api, (6) uploading things to the media library, (7) exporting locale.	8.8	More Details
CVE-2020-35701	An issue was discovered in Cacti 1.2.x through 1.2.16. A SQL injection vulnerability in data_debug.php allows remote authenticated attackers to execute arbitrary SQL commands via the site_id parameter. This can lead to remote code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21116	Heap buffer overflow in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21114	Use after free in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21113	Heap buffer overflow in Skia in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21112	Use after free in Blink in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16043	Insufficient data validation in networking in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to bypass discretionary access control via malicious network traffic.	8.8	More Details
CVE-2020-16039	Use after free in extensions in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16038	Use after free in media in Google Chrome on OS X prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16037	Use after free in clipboard in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16035	Insufficient data validation in cros-disks in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to bypass noexec restrictions via a malicious file.	8.8	More Details
CVE-2020-35654	In Pillow before 8.1.0, TiffDecode has a heap-based buffer overflow when decoding crafted YCbCr files because of certain interpretation conflicts with LibTIFF in RGBA mode.	8.8	More Details
CVE-2020-16028	Heap buffer overflow in WebRTC in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-5805	In Marvell QConvergeConsole GUI <= 5.5.0.74, credentials are stored in cleartext in tomcat-users.xml. OS-level users on the QCC host who are not authorized to use QCC may use the plaintext credentials to login to QCC.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16026	Use after free in WebRTC in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16023	Use after free in WebCodecs in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16022	Insufficient policy enforcement in networking in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially bypass firewall controls via a crafted HTML page.	8.8	More Details
CVE-2020-16020	Inappropriate implementation in cryptohome in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to bypass discretionary access control via a malicious file.	8.8	More Details
CVE-2020-16019	Inappropriate implementation in filesystem in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to bypass noexec restrictions via a malicious file.	8.8	More Details
CVE-2020-16015	Insufficient data validation in WASM in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16013	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.198 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21449	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21450	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PSD file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21451	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated SGI file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2021-21452	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated GIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21453	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated RLE file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	8.8	More Details
CVE-2020-26971	Certain blit values provided by the user were not properly constrained leading to a heap buffer overflow on some video drivers. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.	8.8	More Details
CVE-2020-26118	In SmartBear Collaborator Server through 13.3.13302, use of the Google Web Toolkit (GWT) API introduces a post-authentication Java deserialization vulnerability. The application's UpdateMemento class accepts a serialized Java object directly from the user without properly sanitizing it. A malicious object can be submitted to the server via an authenticated attacker to execute commands on the underlying system.	8.8	More Details
CVE-2020-8884	rcdsvc in the Proofpoint Insider Threat Management Windows Agent (formerly ObserveIT Windows Agent) before 7.9 allows remote authenticated users to execute arbitrary code as SYSTEM because of improper deserialization over named pipes.	8.8	More Details
CVE-2021-1707	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-26996	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing of CG4 files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12027)	8.8	More Details
CVE-2020-26995	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing of SGI and RGB files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11992)	8.8	More Details
CVE-2020-26994	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing of PCX files. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26991	A vulnerability has been identified in JT2Go (All versions < V13.1.0.2), Teamcenter Visualization (All versions < V13.1.0.2). Affected applications lack proper validation of user-supplied data when parsing ASM files. This could lead to pointer dereferences of a value obtained from untrusted source. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11899)	8.8	More Details
CVE-2020-26990	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing ASM files. A crafted ASM file could trigger a type confusion condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11897)	8.8	More Details
CVE-2020-26988	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11891)	8.8	More Details
CVE-2020-26987	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing of TGA files. This could lead to a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12016, ZDI-CAN-12017)	8.8	More Details
CVE-2021-1700	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-26986	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing of JT files. This could lead to a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12014)	8.8	More Details
CVE-2020-26985	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing of RGB and SGI files. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11986, ZDI-CAN-11994)	8.8	More Details
CVE-2020-26984	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing of JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11972)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26983	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing PDF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11900)	8.8	More Details
CVE-2020-26982	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing CG4 and CGM files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11898)	8.8	More Details
CVE-2020-26980	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing JT files. A crafted JT file could trigger a type confusion condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11881)	8.8	More Details
CVE-2021-1701	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-3121	An issue was discovered in GoGo Protobuf before 1.3.2. plugin/unmarshal/unmarshal.go lacks certain index validation, aka the "skippy peanut butter" issue.	8.6	More Details
CVE-2021-1051	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which a local user can get elevated privileges to modify display configuration data, which may result in denial of service of the display.	8.4	More Details
CVE-2018-20315	Foxit Reader before 9.5, and PhantomPDF before 8.3.10 and 9.x before 9.5, has a race condition that can cause a stack-based buffer overflow or an out-of-bounds read.	8.1	More Details
CVE-2018-20314	Foxit Reader before 9.5, and PhantomPDF before 8.3.10 and 9.x before 9.5, has a proxyCheckLicence race condition that can cause a stack-based buffer overflow or an out-of-bounds read.	8.1	More Details
CVE-2018-20313	Foxit Reader before 9.5, and PhantomPDF before 8.3.10 and 9.x before 9.5, has a proxyPreviewAction race condition that can cause a stack-based buffer overflow or an out-of-bounds read.	8.1	More Details
CVE-2018-20316	Foxit Reader before 9.5, and PhantomPDF before 8.3.10 and 9.x before 9.5, has a proxyDoAction race condition that can cause a stack-based buffer overflow or an out-of-bounds read, a different issue than CVE-2018-20310 because of a different opcode.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28468	This affects the package pwntools before 4.3.1. The shellcraft generator for affected versions of this module are vulnerable to Server-Side Template Injection (SSTI), which can lead to remote code execution.	8.1	More Details
CVE-2020-16041	Out of bounds read in networking in Google Chrome prior to 87.0.4280.88 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page.	8.1	More Details
CVE-2018-20311	Foxit Reader before 9.5, and PhantomPDF before 8.3.10 and 9.x before 9.5, has a proxyCPDFAction race condition that can cause a stack-based buffer overflow or an out-of-bounds read.	8.1	More Details
CVE-2020-36188	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.newrelic.agent.deps.ch.qos.logback.core.db.JNDIConnectionSource.	8.1	More Details
CVE-2020-5804	Marvell QConvergeConsole GUI <= 5.5.0.74 is affected by a path traversal vulnerability. The deleteEventLogFile method of the GWTTestServiceImpl class lacks proper validation of a user-supplied path prior to using it in file deletion operations. An authenticated, remote attacker can leverage this vulnerability to delete arbitrary remote files as SYSTEM or root.	8.1	More Details
CVE-2018-20312	Foxit Reader before 9.5, and PhantomPDF before 8.3.10 and 9.x before 9.5, has a proxyDoAction race condition that can cause a stack-based buffer overflow or an out-of-bounds read, a different issue than CVE-2018-20310 because of a different opcode.	8.1	More Details
CVE-2020-36187	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.datasources.SharedPoolDataSource.	8.1	More Details
CVE-2018-20310	Foxit Reader before 9.5, and PhantomPDF before 8.3.10 and 9.x before 9.5, has a proxyDoAction race condition that can cause a stack-based buffer overflow or an out-of-bounds read.	8.1	More Details
CVE-2018-20309	Foxit Reader before 9.5, and PhantomPDF before 8.3.10 and 9.x before 9.5, has a proxyGetAppEdition race condition that can cause a stack-based buffer overflow or an out-of-bounds read.	8.1	More Details
CVE-2020-36189	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.newrelic.agent.deps.ch.qos.logback.core.db.DriverManagerConnectionSource.	8.1	More Details
CVE-2020-36179	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to oadd.org.apache.commons.dbcp.cpdsadapter.DriverAdapterCPDS.	8.1	More Details
CVE-2020-36180	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.dbcp2.cpdsadapter.DriverAdapterCPDS.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36182	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.cpdsadapter.DriverAdapterCPDS.	8.1	More Details
CVE-2020-36183	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.docx4j.org.apache.xalan.lib.sql.JNDIConnectionPool.	8.1	More Details
CVE-2020-36186	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.datasources.PerUserPoolDataSource.	8.1	More Details
CVE-2020-36185	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.datasources.SharedPoolDataSource.	8.1	More Details
CVE-2020-8265	Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 are vulnerable to a use-after-free bug in its TLS implementation. When writing to a TLS enabled socket, node::StreamBase::Write calls node::TLSWrap::DoWrite with a freshly allocated WriteWrap object as first argument. If the DoWrite method does not return an error, this object is passed back to the caller as part of a StreamWriteResult structure. This may be exploited to corrupt memory leading to a Denial of Service or potentially other exploits.	8.1	More Details
CVE-2020-36184	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.datasources.PerUserPoolDataSource.	8.1	More Details
CVE-2020-36181	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.cpdsadapter.DriverAdapterCPDS.	8.1	More Details
CVE-2021-1712	Microsoft SharePoint Elevation of Privilege Vulnerability	8.0	More Details
CVE-2021-1718	Microsoft SharePoint Server Tampering Vulnerability	8.0	More Details
CVE-2021-1719	Microsoft SharePoint Elevation of Privilege Vulnerability	8.0	More Details
CVE-2020-13545	An exploitable signed conversion vulnerability exists in the TextMaker document parsing functionality of SoftMaker Office 2021's TextMaker application. A specially crafted document can cause the document parser to miscalculate a length used to allocate a buffer, later upon usage of this buffer the application will write outside its bounds resulting in a heap-based memory corruption. An attacker can entice the victim to open a document to trigger this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26664	A vulnerability in EbmlTypeDispatcher::send in VideoLAN VLC media player 3.0.11 allows attackers to trigger a heap-based buffer overflow via a crafted .mkv file.	7.8	More Details
CVE-2020-27275	Delta Electronics DOPSoft Version 4.0.8.21 and prior is vulnerable to an out-of-bounds write while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2020-26989	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Solid Edge SE2020 (All Versions < SE2020MP12), Solid Edge SE2021 (All Versions < SE2021MP2), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11892)	7.8	More Details
CVE-2020-28383	A vulnerability has been identified in JT2Go (All versions < V13.1.0.1), Solid Edge SE2020 (All Versions < SE2020MP12), Solid Edge SE2021 (All Versions < SE2021MP2), Teamcenter Visualization (All versions < V13.1.0.1). Affected applications lack proper validation of user-supplied data when parsing PAR files. This can result in an out of bounds write past the memory location that is a read only image address. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11885)	7.8	More Details
CVE-2020-27277	Delta Electronics DOPSoft Version 4.0.8.21 and prior has a null pointer dereference issue while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2018-11010	A Buffer Overflow issue was discovered in K7Computing K7AntiVirus Premium 15.01.00.53.	7.8	More Details
CVE-2018-11009	A Buffer Overflow issue was discovered in K7Computing K7AntiVirus Premium 15.01.00.53.	7.8	More Details
CVE-2020-35483	AnyDesk before 6.1.0 on Windows, when run in portable mode on a system where the attacker has write access to the application directory, allows this attacker to compromise a local user account via a read-only setting for a Trojan horse gcapi.dll file.	7.8	More Details
CVE-2020-27059	In onAuthenticated of AuthenticationClient.java, there is a possible tapjacking attack when requesting the user's fingerprint due to an overlaid window. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-8.0, Android-8.1, Android-9, Android-10, 11; Android ID: A-159249069.	7.8	More Details
CVE-2020-27281	A stack-based buffer overflow may exist in Delta Electronics CNCSoft ScreenEditor versions 1.01.26 and prior when processing specially crafted project files, which may allow an attacker to execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27287	Delta Electronics CNCSoft-B Versions 1.0.0.2 and prior is vulnerable to an out-of-bounds write while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2020-27289	Delta Electronics CNCSoft-B Versions 1.0.0.2 and prior has a null pointer dereference issue while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2020-28384	A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP12), Solid Edge SE2021 (All Versions < SE2021MP2). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could lead to a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2020-27293	Delta Electronics CNCSoft-B Versions 1.0.0.2 and prior has a type confusion issue while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-3134	Mubu 2.2.1 allows local users to gain privileges to execute commands, aka CNVD-2020-68878.	7.8	More Details
CVE-2020-27291	Delta Electronics CNCSoft-B Versions 1.0.0.2 and prior is vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2018-8044	K7Computing Pvt Ltd K7Antivirus Premium 15.1.0.53 is affected by: Incorrect Access Control. The impact is: Local Process Execution (local). The component is: K7Sentry.sys.	7.8	More Details
CVE-2018-8724	K7Computing Pvt Ltd K7AntiVirus Premium 15.1.0.53 is affected by: Incorrect Access Control. The impact is: gain privileges (local). The component is: K7TSMngr.exe.	7.8	More Details
CVE-2020-26992	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing CGM files. This could lead to a stack based buffer overflow while trying to copy to a buffer during font string handling. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2020-35459	An issue was discovered in ClusterLabs crmsh through 4.2.1. Local attackers able to call "crm history" (when "crm" is run) were able to execute commands via shell code injection to the crm history commandline, potentially allowing escalation of privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0306	In addAllPermissions of PermissionManagerService.java, there is a possible permissions bypass when upgrading major Android versions which allows an app to gain the android.permission.ACTIVITY_RECOGNITION permission without user confirmation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11, Android-8.0, Android-8.1, Android-9, Android-10; Android ID: A-154505240.	7.8	More Details
CVE-2021-0307	In updatePermissionSourcePackage of PermissionManagerService.java, there is a possible automatic runtime permission grant due to a confused deputy. This could lead to local escalation of privilege allowing a malicious app to silently gain access to a dangerous permission with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-10, Android-11; Android ID: A-155648771.	7.8	More Details
CVE-2021-0310	In LazyServiceRegistrar of LazyServiceRegistrar.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Android ID: A-170212632.	7.8	More Details
CVE-2020-28382	A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP12), Solid Edge SE2021 (All Versions < SE2021MP2). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in a out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-0317	In createOrUpdate of Permission.java and related code, there is possible permission escalation due to a logic error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-10, Android-11, Android-8.0, Android-8.1, Android-9; Android ID: A-168319670.	7.8	More Details
CVE-2020-28386	A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP12), Solid Edge SE2021 (All Versions < SE2021MP2). Affected applications lack proper validation of user-supplied data when parsing DFT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-0318	In appendEventsToCacheLocked of SensorEventConnection.cpp, there is a possible out of bounds write due to a use-after-free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-9, Android-8.1, Android-10, Android-11; Android ID: A-168211968.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28381	A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP12), Solid Edge SE2021 (All Versions < SE2021MP2). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write into uninitialized memory. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2018-9333	K7Computing Pvt Ltd K7AntiVirus Premium 15.1.0.53 is affected by: Buffer Overflow. The impact is: execute arbitrary code (local). The component is: K7TSMngr.exe.	7.8	More Details
CVE-2018-9332	K7Computing Pvt Ltd K7AntiVirus Premium 15.01.00.53 is affected by: Incorrect Access Control. The impact is: gain privileges (local).	7.8	More Details
CVE-2020-13544	An exploitable sign extension vulnerability exists in the TextMaker document parsing functionality of SoftMaker Office 2021's TextMaker application. A specially crafted document can cause the document parser to sign-extend a length used to terminate a loop, which can later result in the loop's index being used to write outside the bounds of a heap buffer during the reading of file data. An attacker can entice the victim to open a document to trigger this vulnerability.	7.8	More Details
CVE-2018-8725	K7Computing Pvt Ltd K7AntiVirus Premium 15.01.00.53 is affected by: Buffer Overflow. The impact is: execute arbitrary code (local). The component is: K7TSMngr.exe.	7.8	More Details
CVE-2020-26050	SaferVPN for Windows Ver 5.0.3.3 through 5.0.4.15 could allow local privilege escalation from low privileged users to SYSTEM via a crafted openssl configuration file. This issue is similar to CVE-2019-12572.	7.8	More Details
CVE-2021-23240	selinux_edit_copy_tfiles in sudoedit in Sudo before 1.9.5 allows a local unprivileged user to gain file ownership and escalate privileges by replacing a temporary file with a symlink to an arbitrary file target. This affects SELinux RBAC support in permissive mode. Machines without SELinux are not vulnerable.	7.8	More Details
CVE-2020-26993	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing CGM files. This could lead to a stack based buffer overflow while trying to copy to a buffer in the font index handling function. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2018-8726	K7Computing Pvt Ltd K7Antivirus Premium 15.1.0.53 is affected by: Buffer Overflow. The impact is: execute arbitrary code (local). The component is: K7TSMngr.exe.	7.8	More Details
CVE-2021-1063	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input offset is not validated, which may lead to a buffer overread, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1653	Windows CSC Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1652	Windows CSC Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1689	Windows Multipoint Management Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1052	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape or IOCTL in which user-mode clients can access legacy privileged APIs, which may lead to denial of service, escalation of privileges, and information disclosure.	7.8	More Details
CVE-2021-1690	Windows WalletService Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1668	Microsoft DTV-DVD Video Decoder Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1649	Active Template Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1650	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1703	Windows Event Logging Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1651	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1716	Microsoft Word Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1693	Windows CSC Service Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1688	Windows CSC Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1702	Windows Remote Procedure Call Runtime Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1695	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1654	Windows CSC Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1655	Windows CSC Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1657	Windows Fax Compose Form Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1659	Windows CSC Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1665	GDI+ Remote Code Execution Vulnerability	7.8	More Details
CVE-2018-19418	Foxit PDF ActiveX before 5.5.1 allows remote code execution via command injection because of the lack of a security permission control.	7.8	More Details
CVE-2021-1661	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1697	Windows InstallService Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1648	Microsoft splwow64 Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1647	Microsoft Defender Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1687	Windows WalletService Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1715	Microsoft Word Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1714	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1713	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1711	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1059	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input index is not validated, which may lead to integer overflow, which in turn may cause tampering of data, information disclosure, or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	7.8	More Details
CVE-2021-1710	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1057	NVIDIA Virtual GPU Manager NVIDIA vGPU manager contains a vulnerability in the vGPU plugin in which it allows guests to allocate some resources for which the guest is not authorized, which may lead to integrity and confidentiality loss, denial of service, or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	7.8	More Details
CVE-2021-1686	Windows WalletService Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1681	Windows WalletService Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1642	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1680	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1643	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1644	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1662	Windows Event Tracing Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-1638	Microsoft is aware of the "Impersonation in the Passkey Entry Protocol" vulnerability. For more information regarding the vulnerability, please see this statement from the Bluetooth SIG. To address the vulnerability, Microsoft has released a software update that will fail attempts to pair if the remote device exchanges a public key with the same X coordinate as the locally exchanged public key	7.7	More Details
CVE-2020-4079	Combodo iTop is a web based IT Service Management tool. In iTop before versions 2.7.2 and 2.8.0, when the ajax endpoint for the "excel export" portal functionality is called directly it allows getting data without scope filtering. This allows a user to access data they which they should not have access to. This is fixed in versions 2.7.2 and 3.0.0.	7.7	More Details
CVE-2021-1692	Windows Hyper-V Denial of Service Vulnerability	7.7	More Details
CVE-2021-1691	Windows Hyper-V Denial of Service Vulnerability	7.7	More Details
CVE-2021-3116	before_upstream_connection in AuthPlugin in http/proxy/auth.py in proxy.py before 2.3.1 accepts incorrect Proxy-Authorization header data because of a boolean confusion (and versus or).	7.5	More Details
CVE-2021-1694	Windows Update Stack Elevation of Privilege Vulnerability	7.5	More Details
CVE-2020-17508	The ATS ESI plugin has a memory disclosure vulnerability. If you are running the plugin please upgrade. Apache Traffic Server versions 7.0.0 to 7.1.11 and 8.0.0 to 8.1.0 are affected.	7.5	More Details
CVE-2020-17509	ATS negative cache option is vulnerable to a cache poisoning attack. If you have this option enabled, please upgrade or disable this feature. Apache Traffic Server versions 7.0.0 to 7.1.11 and 8.0.0 to 8.1.0 are affected.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-11246	K7TSMngr.exe in K7Computing K7AntiVirus Premium 15.1.0.53 has a Memory Leak.	7.5	More Details
CVE-2021-1723	ASP.NET Core and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2020-13559	A denial-of-service vulnerability exists in the traffic-logging functionality of FreyrSCADA IEC-60879-5-104 Server Simulator 21.04.028. A specially crafted packet can lead to denial of service. An attacker can send a malicious packet to trigger this vulnerability.	7.5	More Details
CVE-2020-16146	Espressif ESP-IDF 2.x, 3.0.x through 3.0.9, 3.1.x through 3.1.7, 3.2.x through 3.2.3, 3.3.x through 3.3.2, and 4.0.x through 4.0.1 has a Buffer Overflow in BluFi provisioning in btc_blufi_recv_handler function in blufi_prf.c. An attacker can send a crafted BluFi protocol Write Attribute command to characteristic 0xFF01. With manipulated packet fields, there is a buffer overflow.	7.5	More Details
CVE-2021-21446	SAP NetWeaver AS ABAP, versions 740, 750, 751, 752, 753, 754, 755, allows an unauthenticated attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service, this has a high impact on the availability of the service.	7.5	More Details
CVE-2021-21469	When security guidelines for SAP NetWeaver Master Data Management running on windows have not been thoroughly reviewed, it might be possible for an external operator to try and set custom paths in the MDS server configuration. When no adequate protection has been enforced on any level (e.g., MDS Server password not set, network and OS configuration not properly secured, etc.), a malicious user might define UNC paths which could then be exploited to put the system at risk using a so-called SMB relay attack and obtain highly sensitive data, which leads to Information Disclosure.	7.5	More Details
CVE-2020-16021	Race in image burner in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to perform OS-level privilege escalation via a malicious file.	7.5	More Details
CVE-2020-24577	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. The One Touch application discloses sensitive information, such as the hashed admin login password and the Internet provider connection username and cleartext password, in the application's response body for a /tmp/var/passwd or /tmp/home/wan_stat URI.	7.5	More Details
CVE-2020-27279	A NULL pointer deference vulnerability has been identified in the protocol converter. An attacker could send a specially crafted packet that could reboot the device running Crimson 3.1 (Build versions prior to 3119.001).	7.5	More Details
CVE-2020-14274	Information disclosure vulnerability in HCL Commerce 9.0.1.9 through 9.0.1.14 and 9.1 through 9.1.4 could allow a remote attacker to obtain user personal data via unknown vectors.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13573	A denial-of-service vulnerability exists in the Ethernet/IP server functionality of Rockwell Automation RSLinx Classic 2.57.00.14 CPR 9 SR 3. A specially crafted network request can lead to a denial of service. An attacker can send a sequence of malicious packets to trigger this vulnerability.	7.5	More Details
CVE-2020-36176	The iThemes Security (formerly Better WP Security) plugin before 7.7.0 for WordPress does not enforce a new-password requirement for an existing account until the second login occurs.	7.5	More Details
CVE-2020-36049	socket.io-parser before 3.4.1 allows attackers to cause a denial of service (memory consumption) via a large packet because a concatenation approach is used.	7.5	More Details
CVE-2020-36048	Engine.IO before 4.0.0 allows attackers to cause a denial of service (resource consumption) via a POST request to the long polling transport.	7.5	More Details
CVE-2020-13449	A directory traversal vulnerability in the Markdown engine of Gotenberg through 6.2.1 allows an attacker to read any container files.	7.5	More Details
CVE-2020-5018	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 may include sensitive information in its URLs increasing the risk of such information being caputured by an attacker. IBM X-Force ID: 193654.	7.5	More Details
CVE-2020-4898	IBM Emptoris Strategic Supply Management 10.1.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 190989.	7.5	More Details
CVE-2021-0313	In isWordBreakAfter of LayoutUtils.cpp, there is a possible way to slow or crash a TextView due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-9, Android-10, Android-11, Android-8.0, Android-8.1; Android ID: A-170968514.	7.5	More Details
CVE-2021-21241	The Python "Flask-Security-Too" package is used for adding security features to your Flask application. It is an is a independently maintained version of Flask-Security based on the 3.0.0 version of Flask-Security. In Flask-Security-Too from version 3.3.0 and before version 3.4.5, the /login and /change endpoints can return the authenticated user's authentication token in response to a GET request. Since GET requests aren't protected with a CSRF token, this could lead to a malicious 3rd party site acquiring the authentication token. Version 3.4.5 and version 4.0.0 are patched. As a workaround, if you aren't using authentication tokens - you can set the SECURITY_TOKEN_MAX_AGE to "0" (seconds) which should make the token unusable.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0319	In checkCallerIsSystemOr of CompanionDeviceManagerService.java, there is a possible way to get a nearby Bluetooth device's MAC address without appropriate permissions due to a permissions bypass. This could lead to local escalation of privilege that grants access to nearby MAC addresses, with User execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-8.0, Android-8.1, Android-9, Android-10, Android-11; Android ID: A-167244818.	7.3	More Details
CVE-2021-1704	Windows Hyper-V Elevation of Privilege Vulnerability	7.3	More Details
CVE-2021-1685	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability	7.3	More Details
CVE-2021-1706	Windows LUAFV Elevation of Privilege Vulnerability	7.3	More Details
CVE-2021-0315	In onCreate of GrantCredentialsPermissionActivity.java, there is a possible way to convince the user to grant an app access to an account due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-8.1, Android-9, Android-10, Android-11, Android-8.0; Android ID: A-169763814.	7.3	More Details
CVE-2020-17504	The NDN-210 has a web administration panel which is made available over https. There is a command injection issue that will allow authenticated users to the administration panel to perform authenticated remote code execution. An issue exists in ngpsystemcmd.php in which the http parameters "x_modules" and "y_modules" are not properly handled. The NDN-210 is part of Barco TransForm N solution and this vulnerability is patched from TransForm N version 3.8 onwards.	7.2	More Details
CVE-2020-2508	A command injection vulnerability has been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. QNAP have already fixed this vulnerability in the following versions: QTS 4.5.1.1456 build 20201015 (and later) QuTS hero h4.5.1.1472 build 20201031 (and later)	7.2	More Details
CVE-2020-28672	MonoCMS Blog 1.0 is affected by incorrect access control that can lead to remote arbitrary code execution. At monofiles/category.php:27, user input can be saved to category/[foldername]/index.php causing RCE.	7.2	More Details
CVE-2020-10657	The Proofpoint Insider Threat Management Server (formerly ObserveIT Server) before 7.9.1 contains a vulnerability in the ITM web console's ImportAlertRules feature. The vulnerability allows a remote attacker (with admin or config-admin privileges in the console) to execute arbitrary code with local administrator privileges. The vulnerability is caused by improper deserialization.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5146	A vulnerability in SonicWall SMA100 appliance allow an authenticated management-user to perform OS command injection using HTTP POST parameters. This vulnerability affected SMA100 Appliance version 10.2.0.2-20sv and earlier.	7.2	More Details
CVE-2020-17502	Barco TransForm N before 3.8 allows Command Injection (issue 2 of 4). The NDN-210 has a web administration panel which is made available over https. There is a command injection issue that will allow authenticated users of the administration panel to perform authenticated remote code execution. An issue exists in split_card_cmd.php in which the http parameters xmodules, ymodules and savelocking are not properly handled. The NDN-210 is part of Barco TransForm N solution and includes the patch from TransForm N version 3.8 onwards.	7.2	More Details
CVE-2020-17503	The NDN-210 has a web administration panel which is made available over https. There is a command injection issue that will allow authenticated users to the administration panel to perform authenticated remote code execution. An issue exists in split_card_cmd.php in which the http parameter "locking" is not properly handled. The NDN-210 is part of Barco TransForm N solution and this vulnerability is patched from TransForm N version 3.8 onwards.	7.2	More Details
CVE-2020-35653	In Pillow before 8.1.0, PcxDecode has a buffer over-read when decoding a crafted PCX file because the user-supplied stride value is trusted for buffer calculations.	7.1	More Details
CVE-2021-1056	NVIDIA GPU Display Driver for Linux, all versions, contains a vulnerability in the kernel mode layer (nvidia.ko) in which it does not completely honor operating system file system permissions to provide GPU device-level isolation, which may lead to denial of service or information disclosure.	7.1	More Details
CVE-2021-1065	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	7.1	More Details
CVE-2020-27148	The TIBCO EBX Add-on for Oracle Hyperion EPM, TIBCO EBX Data Exchange Add-on, and TIBCO EBX Insight Add-on components of TIBCO Software Inc.'s TIBCO EBX Add-ons contain a vulnerability that theoretically allows a low privileged attacker with network access to execute an XML External Entity (XXE) attack. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions 4.4.2 and below.	7.1	More Details
CVE-2021-1058	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input data size is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1064	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which it obtains a value from an untrusted source, converts this value to a pointer, and dereferences the resulting pointer, which may lead to information disclosure or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	7.1	More Details
CVE-2021-1060	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and vGPU plugin, in which an input index is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	7.1	More Details
CVE-2021-1062	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which an input data length is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	7.1	More Details
CVE-2021-1709	Windows Win32k Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-0303	In dispatchGraphTerminationMessage() of packages/services/Car/computepipe/runner/graph/StreamSetObserver.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Android ID: A-170407229.	7.0	More Details
CVE-2020-17534	There exists a race condition between the deletion of the temporary file and the creation of the temporary directory in `webkit` subproject of HTML/Java API version 1.7. A similar vulnerability has recently been disclosed in other Java projects and the fix in HTML/Java API version 1.7.1 follows theirs: To avoid local privilege escalation version 1.7.1 creates the temporary directory atomically without dealing with the temporary file: https://github.com/apache/netbeans-html4j/commit/fa70e507e5555e1adb4f6518479fc408a7abd0e6	7.0	More Details
CVE-2021-1682	Windows Kernel Elevation of Privilege Vulnerability	7.0	More Details
CVE-2020-26298	Redcarpet is a Ruby library for Markdown processing. In Redcarpet before version 3.5.1, there is an injection vulnerability which can enable a cross-site scripting attack. In affected versions no HTML escaping was being performed when processing quotes. This applies even when the `:escape_html` option was being used. This is fixed in version 3.5.1 by the referenced commit.	6.8	More Details
CVE-2021-0308	In ReadLogicalParts of basicmbr.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-8.1, Android-9, Android-10, Android-11, Android-8.0; Android ID: A-158063095.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26186	Dell Inspiron 5675 BIOS versions prior to 1.4.1 contain a UEFI BIOS RuntimeServices overwrite vulnerability. A local attacker with access to system memory may exploit this vulnerability by overwriting the RuntimeServices structure to execute arbitrary code in System Management Mode (SMM).	6.8	More Details
CVE-2021-0301	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android SoC; Android ID: A-172514667.	6.7	More Details
CVE-2021-0342	In tun_get_user of tun.c, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges required. User interaction is not required for exploitation. Product: Android; Versions: Android kernel; Android ID: A-146554327.	6.7	More Details
CVE-2021-1646	Windows WLAN Service Elevation of Privilege Vulnerability	6.6	More Details
CVE-2020-5019	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. By sending a specially crafted HTTP request, a remote attacker could exploit this vulnerability to inject HTTP HOST header, which will allow the attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 193655.	6.5	More Details
CVE-2020-26977	By attempting to connect a website using an unresponsive port, an attacker could have controlled the content of a tab while the URL bar displayed the original domain. *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 84.	6.5	More Details
CVE-2021-0311	In ElementaryStreamQueue::dequeueAccessUnitH264() of ESQueue.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-9, Android-10, Android-11, Android-8.0, Android-8.1; Android ID: A-170240631.	6.5	More Details
CVE-2020-4896	IBM Emptoris Sourcing 10.1.0, 10.1.1, and 10.1.3 is vulnerable to web cache poisoning, caused by improper input validation by modifying HTTP request headers. IBM X-Force ID: 190987.	6.5	More Details
CVE-2021-0312	In WAVSource::read of WAVExtractor.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-8.1, Android-9, Android-10, Android-11, Android-8.0; Android ID: A-170583712.	6.5	More Details
CVE-2020-16042	Uninitialized Use in V8 in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16040	Insufficient data validation in V8 in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	6.5	More Details
CVE-2020-16036	Inappropriate implementation in cookies in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to bypass cookie restrictions via a crafted HTML page.	6.5	More Details
CVE-2021-3133	The Elementor Contact Form DB plugin before 1.6 for WordPress allows CSRF via backend admin pages.	6.5	More Details
CVE-2021-21471	In CLA-Assistant, versions before 2.8.5, due to improper access control an authenticated user could access API endpoints which are not intended to be used by the user. This could impact the integrity of the application.	6.5	More Details
CVE-2021-21468	The BW Database Interface does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges that allows the user to practically read out any database table.	6.5	More Details
CVE-2020-16027	Insufficient policy enforcement in developer tools in Google Chrome prior to 87.0.4280.66 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from the user's disk via a crafted Chrome Extension.	6.5	More Details
CVE-2020-26976	When a HTTPS pages was embedded in a HTTP page, and there was a service worker registered for the former, the service worker could have intercepted the request for the secure page despite the iframe not being a secure context due to the (insecure) framing. This vulnerability affects Firefox < 84.	6.5	More Details
CVE-2020-26975	When a malicious application installed on the user's device broadcast an Intent to Firefox for Android, arbitrary headers could have been specified, leading to attacks such as abusing ambient authority or session fixation. This was resolved by only allowing certain safe-listed headers. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 84.	6.5	More Details
CVE-2021-21448	SAP GUI for Windows, version - 7.60, allows an attacker to spoof logon credentials for Application Server ABAP backend systems in the client PCs memory. Under certain conditions the attacker can access information which would otherwise be restricted. The exploit can only be executed locally on the client PC and not via Network and the attacker needs at least user authorization of the Operating System user of the victim.	6.5	More Details
CVE-2020-8287	Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 allow two copies of a header field in an HTTP request (for example, two Transfer-Encoding header fields). In this case, Node.js identifies the first header field and ignores the second. This can lead to HTTP Request Smuggling.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36174	The Ninja Forms plugin before 3.4.27.1 for WordPress allows CSRF via services integration.	6.5	More Details
CVE-2020-26981	A vulnerability has been identified in JT2Go (All versions < V13.1.0), Teamcenter Visualization (All versions < V13.1.0). When opening a specially crafted xml file, the application could disclose arbitrary files to remote attackers. This is because of the passing of specially crafted content to the underlying XML parser without taking proper restrictions such as prohibiting an external dtd. (ZDI-CAN-11890)	6.5	More Details
CVE-2020-15799	A vulnerability has been identified in SCALANCE X-200 switch family (incl. SIPLUS NET variants) (All versions < V5.2.5), SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) (All versions < V5.5.0). The vulnerability could allow an unauthenticated attacker to reboot the device over the network by using special urls from integrated web server of the affected products.	6.5	More Details
CVE-2020-35722	CSRF in Web Compliance Manager in Quest Policy Authority 8.1.2.200 allows remote attackers to force user modification/creation via a specially crafted link to the submitUser.jsp file. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.5	More Details
CVE-2020-8274	Citrix Secure Mail for Android before 20.11.0 suffers from Improper Control of Generation of Code ('Code Injection') by allowing unauthenticated access to read data stored within Secure Mail. Note that a malicious app would need to be installed on the Android device or a threat actor would need to execute arbitrary code on the Android device.	6.5	More Details
CVE-2020-13922	Versions of Apache DolphinScheduler prior to 1.3.2 allowed an ordinary user under any tenant to override another users password through the API interface.	6.5	More Details
CVE-2020-4869	IBM MQ Appliance 9.2 CD and 9.2 LTS is vulnerable to a denial of service, caused by a buffer overflow. A remote attacker could send a specially crafted SNMP query to cause the appliance to reload. IBM X-Force ID: 190831.	6.5	More Details
CVE-2021-1679	Windows CryptoAPI Denial of Service Vulnerability	6.5	More Details
CVE-2021-23927	OX App Suite through 7.10.4 allows SSRF via a URL with an @ character in an appsuite/api/oauth/proxy PUT request.	6.4	More Details
CVE-2021-1061	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which a race condition may cause the vGPU plugin to continue using a previously validated resource that has since changed, which may lead to denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23933	OX App Suite through 7.10.4 allows XSS via JavaScript in a Note referenced by a mail:// URL.	6.1	More Details
CVE-2021-23932	OX App Suite through 7.10.4 allows XSS via an inline image with a crafted filename.	6.1	More Details
CVE-2021-23931	OX App Suite through 7.10.4 allows XSS via an inline binary file.	6.1	More Details
CVE-2021-23934	OX App Suite through 7.10.4 allows XSS via a contact whose name contains JavaScript code.	6.1	More Details
CVE-2021-23930	OX App Suite through 7.10.4 allows XSS via use of the conversion API for a distributedFile.	6.1	More Details
CVE-2021-23935	OX App Suite through 7.10.4 allows XSS via an appointment in which the location contains JavaScript code.	6.1	More Details
CVE-2021-23929	OX App Suite through 7.10.4 allows XSS via a crafted Content-Disposition header in an uploaded HTML document to an ajax/share/<share-token>?delivery=view URI.	6.1	More Details
CVE-2021-23928	OX App Suite through 7.10.3 allows XSS via the ajax/apps/manifests query string.	6.1	More Details
CVE-2021-23125	An issue was discovered in Joomla! 3.1.0 through 3.9.23. The lack of escaping of image-related parameters in multiple com_tags views cause lead to XSS attack vectors.	6.1	More Details
CVE-2021-23124	An issue was discovered in Joomla! 3.9.0 through 3.9.23. The lack of escaping in mod_breadcrumbs aria-label attribute allows XSS attacks.	6.1	More Details
CVE-2020-36172	The Advanced Custom Fields plugin before 5.8.12 for WordPress mishandles the escaping of strings in Select2 dropdowns, potentially leading to XSS.	6.1	More Details
CVE-2020-36190	RailsAdmin (aka rails_admin) before 1.4.3 and 2.x before 2.0.2 allows XSS via nested forms.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23849	Stored XSS was discovered in the tree mode of jsoneditor before 9.0.2 through injecting and executing JavaScript.	6.1	More Details
CVE-2020-36171	The Elementor Website Builder plugin before 3.0.14 for WordPress does not properly restrict SVG uploads.	6.1	More Details
CVE-2020-26768	Formstone <=1.4.16 is vulnerable to a Reflected Cross-Site Scripting (XSS) vulnerability caused by improper validation of user supplied input in the upload-target.php and upload-chunked.php files. A remote attacker could exploit this vulnerability using a specially crafted URL to execute a script in a victim's Web browser within the security context of the hosting Web site once the URL is clicked or visited. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials, force malware execution, user redirection and others.	6.1	More Details
CVE-2020-8160	MendixSSO <= 2.1.1 contains endpoints that make use of the openid handler, which is suffering from a Cross-Site Scripting vulnerability via the URL path. This is caused by the reflection of user-supplied data without appropriate HTML escaping or output encoding. As a result, a JavaScript payload may be injected into the above endpoint causing it to be executed within the context of the victim's browser.	6.1	More Details
CVE-2020-25476	Liferay CMS Portal version 7.1.3 and 7.2.1 have a blind persistent cross-site scripting (XSS) vulnerability in the user name parameter to Calendar. An attacker can insert the malicious payload on the username, lastname or surname fields of its own profile, and the malicious payload will be injected and reflected in the calendar of the user who submitted the payload. An attacker could escalate its privileges in case an admin visits the calendar that injected the payload.	6.1	More Details
CVE-2020-8264	In actionpack gem >= 6.0.0, a possible XSS vulnerability exists when an application is running in development mode allowing an attacker to send or embed (in another page) a specially crafted URL which can allow the attacker to execute JavaScript in the context of the local application. This vulnerability is in the Actionable Exceptions middleware.	6.1	More Details
CVE-2020-35262	Cross Site Scripting (XSS) vulnerability in Digisol DG-HR3400 can be exploited via the NTP server name in Time and date module and "Keyword" in URL Filter.	6.1	More Details
CVE-2020-26979	When a user typed a URL in the address bar or the search bar and quickly hit the enter key, a website could sometimes capture that event and then redirect the user before navigation occurred to the desired, entered address. To construct a convincing spoof the attacker would have had to guess what the user was typing, perhaps by suggesting it. This vulnerability affects Firefox < 84.	6.1	More Details
CVE-2020-24900	The default installation of Krpano Panorama Viewer version <=1.20.8 is prone to Reflected XSS due to insecure XML load in file /viewer/krpano.html, parameter xml.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24901	The default installation of Krpano Panorama Viewer version <=1.20.8 is vulnerable to Reflected XSS due to insecure remote js load in file viewer/krpano.html, parameter plugin[test].url.	6.1	More Details
CVE-2020-26978	Using techniques that built on the slipstream research, a malicious webpage could have exposed both an internal network's hosts as well as services running on the user's local machine. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.	6.1	More Details
CVE-2020-24903	Cute Editor for ASP.NET 6.4 is vulnerable to reflected cross-site scripting (XSS) caused by improper validation of user supplied input. A remote attacker could exploit this vulnerability using a specially crafted URL to execute a script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.	6.1	More Details
CVE-2020-23644	XSS exists in JIZHICMS 1.7.1 via index.php/Error/index?msg={XSS] to Home/c/ErrorController.php.	6.1	More Details
CVE-2021-23936	OX App Suite through 7.10.4 allows XSS via the subject of a task.	6.1	More Details
CVE-2020-16030	Insufficient data validation in Blink in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.	6.1	More Details
CVE-2020-35203	Reflected XSS in Web Compliance Manager in Quest Policy Authority version 8.1.2.200 allows attackers to inject malicious code into the browser via a specially crafted link to the initFile.jsp file via the msg parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details
CVE-2020-24701	OX App Suite through 7.10.4 allows XSS via the app loading mechanism (the PATH_INFO to the /appsuite URI).	6.1	More Details
CVE-2020-35725	Reflected XSS in Quest Policy Authority 8.1.2.200 allows remote attackers to inject malicious code into the browser via a specially crafted link to the /WebCM/index.jsp file via the msg parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details
CVE-2020-35726	Reflected XSS in Quest Policy Authority 8.1.2.200 allows remote attackers to inject malicious code into the browser via a specially crafted link to the /WebCM/Applications/Reports/index.jsp file via the by parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details
CVE-2020-23631	Cross-site request forgery (CSRF) in admin/global/manage.php in WDJA CMS 1.5 allows remote attackers to conduct cross-site scripting (XSS) attacks via the tongji parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35719	Reflected XSS in Quest Policy Authority 8.1.2.200 allows remote attackers to inject malicious code into the browser via a specially crafted link to the /WebCM/Applications/Search/index.jsp file via the added parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details
CVE-2020-26713	REDCap 10.3.4 contains a XSS vulnerability in the ToDoList function with parameter sort. The information submitted by the user is immediately returned in the response and not escaped leading to the reflected XSS vulnerability. Attackers can exploit vulnerabilities to steal login session information or borrow user rights to perform unauthorized acts.	6.1	More Details
CVE-2020-35206	Reflected XSS in Web Compliance Manager in Quest Policy Authority version 8.1.2.200 allows attackers to inject malicious code into the browser via a specially crafted link to the cConn.jsp file via the ur parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details
CVE-2020-5020	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 193656.	6.1	More Details
CVE-2020-23643	XSS exists in JIZHICMS 1.7.1 via index.php/Wechat/checkWeixin?signature=1&echostr={XSS] to Home/c/WechatController.php.	6.1	More Details
CVE-2020-35204	Reflected XSS in Quest Policy Authority version 8.1.2.200 allows attackers to inject malicious code into the browser via a specially crafted link to the PolicyAuthority/Common/FolderControl.jsp file via the unqID parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details
CVE-2020-28391	A vulnerability has been identified in SCALANCE X-200 switch family (incl. SIPLUS NET variants) (All versions < V5.2.5), SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) (All versions < V5.5.0), SCALANCE X-200RNA switch family (All versions < V3.2.7). Devices create a new unique key upon factory reset, except when used with C-PLUG. When used with C-PLUG the devices use the hardcoded private RSA-key shipped with the firmware-image. An attacker could leverage this situation to a man-in-the-middle situation and decrypt previously captured traffic.	5.9	More Details
CVE-2020-25659	python-cryptography 3.2 is vulnerable to Bleichenbacher timing attacks in the RSA decryption API, via timed processing of valid PKCS#1 v1.5 ciphertext.	5.9	More Details
CVE-2020-25657	A flaw was found in all released versions of m2crypto, where they are vulnerable to Bleichenbacher timing attacks in the RSA decryption API via the timed processing of valid PKCS#1 v1.5 Ciphertext. The highest threat from this vulnerability is to confidentiality.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28395	A vulnerability has been identified in SCALANCE X-200RNA switch family (All versions < V3.2.7), SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants) (All versions < V4.1.0). Devices do not create a new unique private key after factory reset. An attacker could leverage this situation to a man-in-the-middle situation and decrypt previously captured traffic.	5.9	More Details
CVE-2020-4893	IBM Emptoris Strategic Supply Management 10.1.0, 10.1.1, and 10.1.3 transmits sensitive information in HTTP GET request parameters. This may lead to information disclosure via man in the middle methods. IBM X-Force ID: 190984.	5.9	More Details
CVE-2020-6656	Eaton's easySoft software v7.xx prior to v7.22 are susceptible to file parsing type confusion remote code execution vulnerability. A malicious entity can execute a malicious code or make the application crash by tricking user upload a malformed .E70 file in the application. The vulnerability arises due to improper validation of user data supplied through E70 file which is causing Type Confusion.	5.8	More Details
CVE-2020-6655	The Eaton's easySoft software v7.xx prior to v7.22 are susceptible to Out-of-bounds remote code execution vulnerability. A malicious entity can execute a malicious code or make the application crash by tricking user to upload the malformed .E70 file in the application. The vulnerability arises due to improper validation and parsing of the E70 file content by the application.	5.8	More Details
CVE-2021-21236	CairoSVG is a Python (pypi) package. CairoSVG is an SVG converter based on Cairo. In CairoSVG before version 2.5.1, there is a regular expression denial of service (REDoS) vulnerability. When processing SVG files, the python package CairoSVG uses two regular expressions which are vulnerable to Regular Expression Denial of Service (REDoS). If an attacker provides a malicious SVG, it can make cairosvg get stuck processing the file for a very long time. This is fixed in version 2.5.1. See Referenced GitHub advisory for more information.	5.7	More Details
CVE-2021-21235	kamadak-exif is an exif parsing library written in pure Rust. In kamadak-exif version 0.5.2, there is an infinite loop in parsing crafted PNG files. Specifically, reader::read_from_container can cause an infinite loop when a crafted PNG file is given. This is fixed in version 0.5.3. No workaround is available. Applications that do not pass files with the PNG signature to Reader::read_from_container are not affected.	5.7	More Details
CVE-2021-1708	Windows GDI+ Information Disclosure Vulnerability	5.7	More Details
CVE-2021-0304	In several functions of GlobalScreenshot.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure of the user's contacts with User execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-10, Android-8.0, Android-8.1, Android-9; Android ID: A-162738636.	5.5	More Details
CVE-2021-1725	Bot Framework SDK Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28390	A vulnerability has been identified in Opcenter Execution Core (V8.2), Opcenter Execution Core (V8.3). The application contains an information leakage vulnerability in the handling of web client sessions. A local attacker who has access to the Web Client Session Storage could disclose the passwords of currently logged-in users.	5.5	More Details
CVE-2021-1672	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-1676	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-1677	Azure Active Directory Pod Identity Spoofing Vulnerability	5.5	More Details
CVE-2021-1670	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-1637	Windows DNS Query Information Disclosure Vulnerability	5.5	More Details
CVE-2020-5017	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 may allow a local user to obtain access to information beyond their intended role and permissions. IBM X-Force ID: 193653.	5.5	More Details
CVE-2021-0309	In onCreate of grantCredentialsPermissionActivity, there is a confused deputy. This could lead to local information disclosure and account access with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-8.1, Android-9, Android-10, Android-11, Android-8.0; Android ID: A-158480899.	5.5	More Details
CVE-2021-1696	Windows Graphics Component Information Disclosure Vulnerability	5.5	More Details
CVE-2021-0321	In enforceDumpPermissionForPackage of ActivityManagerService.java, there is a possible way to determine if a package is installed due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Android ID: A-166667403.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1054	NVIDIA GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which the software does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action, which may lead to denial of service.	5.5	More Details
CVE-2021-1053	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape or IOCTL in which improper validation of a user pointer may lead to denial of service.	5.5	More Details
CVE-2020-26800	A stack overflow vulnerability in Aleth Ethereum C++ client version <= 1.8.0 using a specially crafted a config.json file may result in a denial of service.	5.5	More Details
CVE-2021-1656	TPM Device Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-1066	NVIDIA vGPU manager contains a vulnerability in the vGPU plugin, in which input data is not validated, which may lead to unexpected consumption of resources, which in turn may lead to denial of service. This affects vGPU version 8.x (prior to 8.6) and version 11.0 (prior to 11.3).	5.5	More Details
CVE-2021-1699	Windows (modem.sys) Information Disclosure Vulnerability	5.5	More Details
CVE-2018-11005	A Memory Leak issue was discovered in K7Computing K7AntiVirus Premium 15.01.00.53.	5.5	More Details
CVE-2018-11006	An Incorrect Access Control issue was discovered in K7Computing K7AntiVirus Premium 15.01.00.53.	5.5	More Details
CVE-2018-11007	A Memory Leak issue was discovered in K7Computing K7AntiVirus Premium 15.01.00.53.	5.5	More Details
CVE-2018-11008	An Incorrect Access Control issue was discovered in K7Computing K7AntiVirus Premium 15.01.00.53.	5.5	More Details
CVE-2021-1663	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4691	IBM Jazz Foundation Products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186698.	5.4	More Details
CVE-2020-4697	IBM Jazz Foundation products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186790.	5.4	More Details
CVE-2020-8281	A missing file type check in Nextcloud Contacts 3.3.0 allows a malicious user to upload malicious SVG files to perform cross-site scripting (XSS) attacks.	5.4	More Details
CVE-2020-8280	A missing file type check in Nextcloud Contacts 3.4.0 allows a malicious user to upload SVG files as PNG files to perform cross-site scripting (XSS) attacks.	5.4	More Details
CVE-2020-4895	IBM Emptoris Strategic Supply Management 10.1.0, 10.1.1, and 10.1.3 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 190986.	5.4	More Details
CVE-2020-4892	IBM Emptoris Contract Management 10.1.3 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: 190979.	5.4	More Details
CVE-2020-4663	IBM Engineering Requirements Quality Assistant On-Premises 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: 186234.	5.4	More Details
CVE-2020-25680	A flaw was found in JBCS httpd in version 2.4.37 SP3, where it uses a back-end worker SSL certificate with the keystore file's ID is 'unknown'. The validation of the certificate whether CN and hostname are matching stopped working and allow connecting to the back-end work. The highest threat from this vulnerability is to data integrity.	5.4	More Details
CVE-2020-4733	IBM Jazz Foundation products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 188127.	5.4	More Details
CVE-2021-21447	SAP BusinessObjects Business Intelligence platform, versions 410, 420, allows an authenticated attacker to inject malicious JavaScript payload into the custom value input field of an Input Control, which can be executed by User who views the relevant application content, which leads to Stored Cross-Site Scripting.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35723	Reflected XSS in Quest Policy Authority 8.1.2.200 allows remote attackers to inject malicious code into the browser via a specially crafted link to the ReportPreview.do file via the referer parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.4	More Details
CVE-2020-24700	OX App Suite through 7.10.3 allows SSRF because GET requests are sent to arbitrary domain names with an initial autoconfig. substring.	5.4	More Details
CVE-2020-4838	IBM API Connect 5.0.0.0 through 5.0.8.10 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 190036.	5.4	More Details
CVE-2020-27262	Innokas Yhtymä Oy Vital Signs Monitor VC150 prior to Version 1.7.15 A stored cross-site scripting (XSS) vulnerability exists in the affected products that allow an attacker to inject arbitrary web script or HTML via the filename parameter to multiple update endpoints of the administrative web interface.	5.4	More Details
CVE-2019-16954	SolarWinds Web Help Desk 12.7.0 allows HTML injection via a Comment in a Help Request ticket.	5.4	More Details
CVE-2020-4664	IBM Engineering Requirements Quality Assistant On-Premises 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: 186235.	5.4	More Details
CVE-2020-35721	Reflected XSS in Quest Policy Authority 8.1.2.200 allows remote attackers to inject malicious code into the browser via a specially crafted link to the BrowseAssets.do file via the title parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.4	More Details
CVE-2020-35727	Reflected XSS in Quest Policy Authority 8.1.2.200 allows remote attackers to inject malicious code into the browser via a specially crafted link to the BrowseDirs.do file via the title parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.4	More Details
CVE-2020-35655	In Pillow before 8.1.0, SGIRleDecode has a 4-byte buffer over-read when decoding crafted SGI RLE image files because offsets and length tables are mishandled.	5.4	More Details
CVE-2020-35724	Reflected XSS in Quest Policy Authority 8.1.2.200 allows remote attackers to inject malicious code into the browser via a specially crafted link to the Error.jsp file via the err parameter (or indirectly via the cpr, tcp, or abs parameter). NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4666	IBM Engineering Requirements Quality Assistant On-Premises 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: 186281.	5.4	More Details
CVE-2020-35720	Stored XSS in Quest Policy Authority 8.1.2.200 allows remote attackers to store malicious code in multiple fields (first name, last name, and logon name) when creating or modifying a user via the submitUser.jsp file. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.4	More Details
CVE-2019-16962	Zoho ManageEngine Desktop Central 10.0.430 allows HTML injection via a modified Report Name in a New Custom Report.	5.4	More Details
CVE-2021-21445	SAP Commerce Cloud, versions - 1808, 1811, 1905, 2005, 2011, allows an authenticated attacker to include invalidated data in the HTTP response Content Type header, due to improper input validation, and sent to a Web user. A successful exploitation of this vulnerability may lead to advanced attacks, including cross-site scripting and page hijacking.	5.4	More Details
CVE-2020-13116	OpenText Carbonite Server Backup Portal before 8.8.7 allows XSS by an authenticated user via policy creation.	5.4	More Details
CVE-2020-29041	A misconfiguration in Web-Sesame 2020.1.1.3375 allows an unauthenticated attacker to download the source code of the application, facilitating its comprehension (code review). Specifically, JavaScript source maps were inadvertently included in the production Webpack configuration. These maps contain sources used to generate the bundle, configuration settings (e.g., API keys), and developers' comments.	5.3	More Details
CVE-2018-18688	The Portable Document Format (PDF) specification does not provide any information regarding the concrete procedure of how to validate signatures. Consequently, an Incremental Saving vulnerability exists in multiple products. When an attacker uses the Incremental Saving feature to add pages or annotations, Body Updates are displayed to the user without any action by the signature-validation logic. This affects Foxit Reader before 9.4 and PhantomPDF before 8.3.9 and 9.x before 9.4. It also affects LibreOffice, Master PDF Editor, Nitro Pro, Nitro Reader, Nuance Power PDF Standard, PDF Editor 6 Pro, PDFelement6 Pro, PDF Studio Viewer 2018, PDF Studio Pro, Perfect PDF 10 Premium, and Perfect PDF Reader.	5.3	More Details
CVE-2021-23123	An issue was discovered in Joomla! 3.0.0 through 3.9.23. The lack of ACL checks in the orderPosition endpoint of com_modules leak names of unpublished and/or inaccessible modules.	5.3	More Details
CVE-2020-28208	An email address enumeration vulnerability exists in the password reset function of Rocket.Chat through 3.9.1.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27260	Innokas Yhtymä Oy Vital Signs Monitor VC150 prior to Version 1.7.15 HL7 v2.x injection vulnerabilities exist in the affected products that allow physically proximate attackers with a connected barcode reader to inject HL7 v2.x segments into specific HL7 v2.x messages via multiple expected parameters.	5.3	More Details
CVE-2020-4897	IBM Emptoris Contract Management and IBM Emptoris Spend Analysis 10.1.0, 10.1.1, and 10.1.3 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: 190988.	5.3	More Details
CVE-2018-18689	The Portable Document Format (PDF) specification does not provide any information regarding the concrete procedure of how to validate signatures. Consequently, a Signature Wrapping vulnerability exists in multiple products. An attacker can use /ByteRange and xref manipulations that are not detected by the signature-validation logic. This affects Foxit Reader before 9.4 and PhantomPDF before 8.3.9 and 9.x before 9.4. It also affects eXpert PDF 12 Ultimate, Expert PDF Reader, Nitro Pro, Nitro Reader, PDF Architect 6, PDF Editor 6 Pro, PDF Experte 9 Ultimate, PDFelement6 Pro, PDF Studio Viewer 2018, PDF Studio Pro, PDF-XChange Editor and Viewer, Perfect PDF 10 Premium, Perfect PDF Reader, Soda PDF, and Soda PDF Desktop.	5.3	More Details
CVE-2020-4336	IBM WebSphere eXtreme Scale 8.6.1 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 177932.	5.3	More Details
CVE-2021-23242	MERCUSYS Mercury X18G 1.0.5 devices allow Directory Traversal via ../ to the UPnP server, as demonstrated by the /../../conf/template/uhttpd.json URI.	5.3	More Details
CVE-2021-23253	Opera Mini for Android below 53.1 displays URL left-aligned in the address field. This allows a malicious attacker to craft a URL with a long domain name, e.g. www.safe.opera.com.attacker.com. With the URL being left-aligned, the user will only see the front part (e.g. www.safe.opera.com…) The exact amount depends on the phone screen size but the attacker can craft a number of different domains and target different phones. Starting with version 53.1 Opera Mini displays long URLs with the top-level domain label aligned to the right of the address field which mitigates the issue.	5.3	More Details
CVE-2020-5147	SonicWall NetExtender Windows client vulnerable to unquoted service path vulnerability, this allows a local attacker to gain elevated privileges in the host operating system. This vulnerability impact SonicWall NetExtender Windows client version 10.2.300 and earlier.	5.3	More Details
CVE-2020-27283	An attacker could send a specially crafted message to Crimson 3.1 (Build versions prior to 3119.001) that could leak arbitrary memory locations.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36175	The Ninja Forms plugin before 3.4.27.1 for WordPress allows attackers to bypass validation via the email field.	5.3	More Details
CVE-2019-3405	In the 3.1.3.64296 and lower version of 360F5, the third party can trigger the device to send a deauth frame by constructing and sending a specific illegal 802.11 Null Data Frame, which will cause other wireless terminals connected to disconnect from the wireless, so as to attack the router wireless by DoS. At present, the vulnerability has been effectively handled, and users can fix the vulnerability after updating the firmware version.	5.3	More Details
CVE-2020-36173	The Ninja Forms plugin before 3.4.28 for WordPress lacks escaping for submissions-table fields.	5.3	More Details
CVE-2021-23241	MERCUSYS Mercury X18G 1.0.5 devices allow Directory Traversal via ../ in conjunction with a loginLess or login.htm URI (for authentication bypass) to the web server, as demonstrated by the /loginLess/../../etc/passwd URI.	5.3	More Details
CVE-2021-1055	NVIDIA GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which improper access control may lead to denial of service and information disclosure.	5.3	More Details
CVE-2020-24025	Certificate validation in node-sass 2.0.0 to 4.14.1 is disabled when requesting binaries even if the user is not specifying an alternative download path.	5.3	More Details
CVE-2020-36170	The Ultimate Member plugin before 2.1.13 for WordPress mishandles hidden name="timestamp" fields in forms.	5.3	More Details
CVE-2020-5022	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 may allow unauthenticated and unauthorized access to VDAP proxy which can result in an attacker obtaining information they are not authorized to access. IBM X-Force ID: 193658.	5.3	More Details
CVE-2021-1683	Microsoft is aware of the "Impersonation in the Passkey Entry Protocol" vulnerability. For more information regarding the vulnerability, please see this statement from the Bluetooth SIG. To address the vulnerability, Microsoft has released a software update that will fail attempts to pair if the remote device exchanges a public key with the same X coordinate as the locally exchanged public key	5.0	More Details
CVE-2021-1684	Microsoft is aware of the "Impersonation in the Passkey Entry Protocol" vulnerability. For more information regarding the vulnerability, please see this statement from the Bluetooth SIG. To address the vulnerability, Microsoft has released a software update that will fail attempts to pair if the remote device exchanges a public key with the same X coordinate as the locally exchanged public key	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1645	Windows Docker Information Disclosure Vulnerability	5.0	More Details
CVE-2021-0322	In onCreate of SlicePermissionActivity.java, there is a possible misleading string displayed due to improper input validation. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.Product: Android; Versions: Android-10, Android-11, Android-9; Android ID: A-159145361.	5.0	More Details
CVE-2020-25498	Cross Site Scripting (XSS) vulnerability in Beetel router 777VR1 can be exploited via the NTP server name in System Time and "Keyword" in URL Filter.	4.8	More Details
CVE-2021-3111	The Express Entries Dashboard in Concrete5 8.5.4 allows stored XSS via the name field of a new data object at an index.php/dashboard/express/entries/view/ URI.	4.8	More Details
CVE-2020-24902	Quixplorer <=2.4.1 is vulnerable to reflected cross-site scripting (XSS) caused by improper validation of user supplied input. A remote attacker could exploit this vulnerability using a specially crafted URL to execute a script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.	4.7	More Details
CVE-2021-0320	In is_device_locked and set_device_locked of keystore_keymaster_enforcement.h, there is a possible bypass of lockscreen requirements for keyguard bound keys due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-10, Android-11; Android ID: A-169933423.	4.7	More Details
CVE-2021-1641	Microsoft SharePoint Server Spoofing Vulnerability	4.6	More Details
CVE-2021-1717	Microsoft SharePoint Server Spoofing Vulnerability	4.6	More Details
CVE-2020-25678	A flaw was found in ceph in versions prior to 16.y.z where ceph stores mgr module passwords in clear text. This can be found by searching the mgr logs for grafana and dashboard, with passwords visible.	4.4	More Details
CVE-2020-27835	A use after free in the Linux kernel infiniband hfi1 driver in versions prior to 5.10-rc6 was found in the way user calls ioctl after open dev file and fork. A local user could use this flaw to crash the system.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21470	SAP EPM Add-in for Microsoft Office, version - 1010 and SAP EPM Add-in for SAP Analysis Office, version - 2.8, allows an authenticated attacker with user privileges to parse malicious XML files which could result in XXE-based attacks in applications that accept attacker-controlled XML configuration files. This occurs as logging service does not disable XML external entities when parsing configuration files and a successful exploit would result in limited impact on integrity and availability of the application.	4.4	More Details
CVE-2020-5021	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 does not invalidate session after a password reset which could allow a local user to impersonate another user on the system. IBM X-Force ID: 193657.	4.4	More Details
CVE-2020-4606	IBM Security Verify Privilege Manager 10.8 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A local attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 184883.	4.4	More Details
CVE-2020-4487	IBM Jazz Foundation Products 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: 181862.	4.3	More Details
CVE-2020-4544	IBM Jazz Foundation Products 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: 183189.	4.3	More Details
CVE-2020-25950	Advanced Webhost Billing System 3.7.0 is affected by Cross Site Request Forgery (CSRF) attacks that can delete a contact from the My Additional Contact page.	4.3	More Details
CVE-2020-8275	Citrix Secure Mail for Android before 20.11.0 suffers from improper access control allowing unauthenticated access to read limited calendar related data stored within Secure Mail. Note that a malicious app would need to be installed on the Android device or a threat actor would need to execute arbitrary code on the Android device.	4.3	More Details
CVE-2020-35111	When an extension with the proxy permission registered to receive <all_urls>, the proxy.onRequest callback was not triggered for view-source URLs. While web content cannot navigate to such URLs, a user opening View Source could have inadvertently leaked their IP address. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.	4.3	More Details
CVE-2020-16012	Side-channel information leakage in graphics in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2020-16033	Inappropriate implementation in WebUSB in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to spoof security UI via a crafted HTML page.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21464	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-16034	Inappropriate implementation in WebRTC in Google Chrome prior to 87.0.4280.66 allowed a local attacker to bypass policy restrictions via a crafted HTML page.	4.3	More Details
CVE-2020-16032	Insufficient data validation in sharing in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	4.3	More Details
CVE-2020-4667	IBM Engineering Requirements Quality Assistant On-Premises could allow an authenticated user to obtain sensitive information due to improper input validation. IBM X-Force ID: 186282.	4.3	More Details
CVE-2021-21467	SAP Banking Services (Generic Market Data) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. An unauthorized User is allowed to display restricted Business Partner Generic Market Data (GMD), due to improper authorization check.	4.3	More Details
CVE-2020-16031	Insufficient data validation in UI in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	4.3	More Details
CVE-2020-4673	IBM Workload Automation 9.5 stores sensitive information in HTML comments that could aid in further attacks against the system. IBM X-Force ID: 186286.	4.3	More Details
CVE-2020-4674	IBM Workload Automation 9.5 stores the server path in URLs that could aid in further attacks against the system. IBM X-Force ID: 186287.	4.3	More Details
CVE-2021-3011	An electromagnetic-wave side-channel issue was discovered on NXP SmartMX / P5x security microcontrollers and A7x secure authentication microcontrollers, with CryptoLib through v2.9. It allows attackers to extract the ECDSA private key after extensive physical access (and consequently produce a clone). This was demonstrated on the Google Titan Security Key, based on an NXP A7005a chip. Other FIDO U2F security keys are also impacted (Yubico YubiKey Neo and Feitian K9, K13, K21, and K40) as well as several NXP JavaCard smartcards (J3A081, J2A081, J3A041, J3D145_M59, J2D145_M59, J3D120_M60, J3D082_M60, J2D120_M60, J2D082_M60, J3D081_M59, J2D081_M59, J3D081_M61, J2D081_M61, J3D081_M59_DF, J3D081_M61_DF, J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, J3E041_M64, J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, J2E082_M65, J3E081_M64_DF, J3E081_M66_DF, J3E041_M66_DF, J3E016_M66_DF, J3E041_M64_DF, and J3E016_M64_DF).	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1705	Microsoft Edge (HTML-based) Memory Corruption Vulnerability	4.2	More Details
CVE-2020-24003	Microsoft Skype through 8.59.0.77 on macOS has the disable-library-validation entitlement, which allows a local process (with the user's privileges) to obtain unprompted microphone and camera access by loading a crafted library and thereby inheriting Skype Client's microphone and camera access.	3.3	More Details
CVE-2020-14341	The "Test Connection" available in v7.x of the Red Hat Single Sign On application console can permit an authorized user to cause SMTP connections to be attempted to arbitrary hosts and ports of the user's choosing, and originating from the RHSSO installation. By observing differences in the timings of these scans, an attacker may glean information about hosts and ports which they do not have access to scan directly.	2.7	More Details
CVE-2021-23239	The sudoedit personality of Sudo before 1.9.5 may allow a local unprivileged user to perform arbitrary directory-existence tests by winning a sudo_edit.c race condition in replacing a user-controlled directory by a symlink to an arbitrary path.	2.5	More Details
CVE-2020-5114	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6680	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5113	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5112	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6741	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5111	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6679	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5110	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6678	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5116	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5115	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5121	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5117	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5118	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5119	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5120	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6681	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6682	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5122	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5123	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5124	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5125	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5126	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5127	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5109	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6677	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5108	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6670	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-16526	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-6660	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6661	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6662	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6663	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6664	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6665	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6666	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6667	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6668	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6669	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6671	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5107	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6672	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6673	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6674	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6675	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6676	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5102	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5103	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5104	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5128	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5105	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5106	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6683	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6684	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6742	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6685	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6719	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6720	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6721	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6722	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6723	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6724	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6725	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6726	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6727	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6728	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6729	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6730	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6731	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6732	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6733	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6734	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6735	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6736	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6737	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6738	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6739	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6740	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6749	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6748	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6747	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6746	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6745	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6744	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6743	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6718	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6717	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6716	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6699	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6686	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6687	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6688	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6689	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6690	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6691	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6692	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6693	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6694	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6695	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6696	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6697	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6698	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6700	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6715	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6701	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6702	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6703	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6704	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6705	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6706	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6707	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6708	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6709	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6710	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6711	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6712	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6714	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6713	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details