SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 15 July 2020

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-1350	A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests, aka 'Windows DNS Server Remote Code Execution Vulnerability'.	10.0	More Details
CVE-2020-6287	SAP NetWeaver AS JAVA (LM Configuration Wizard), versions - 7.30, 7.31, 7.40, 7.50, does not perform an authentication check which allows an attacker without prior authentication to execute configuration tasks to perform critical actions against the SAP Java system, including the ability to create an administrative user, and therefore compromising Confidentiality, Integrity and Availability of the system, leading to Missing Authentication Check.	10.0	More Details
CVE-2020-13753	The bubblewrap sandbox of WebKitGTK and WPE WebKit, prior to 2.28.3, failed to properly block access to CLONE_NEWUSER and the TIOCSTI ioctl. CLONE_NEWUSER could potentially be used to confuse xdg-desktop-portal, which allows access outside the sandbox. TIOCSTI can be used to directly execute commands outside the sandbox by writing to the controlling terminal's input buffer, similar to CVE-2017-5226.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1025	An elevation of privilege vulnerability exists when Microsoft SharePoint Server and Skype for Business Server improperly handle OAuth token validation. An attacker who successfully exploited the vulnerability could bypass authentication and achieve improper access. To exploit this vulnerability, an attacker would need to modify the token. The update addresses the vulnerability by modifying how Microsoft SharePoint Server and Skype for Business Server validate tokens.	9.8	More Details
CVE-2020-9297	Netflix Titus, all versions prior to version v0.1.1-rc.274, uses Java Bean Validation (JSR 380) custom constraint validators. When building custom constraint violation error messages, different types of interpolation are supported, including Java EL expressions. If an attacker can inject arbitrary data in the error message template being passed to ConstraintValidatorContext.buildConstraintViolationWithTemplate() argument, they will be able to run arbitrary Java code.	9.8	More Details
CVE-2020-11546	SuperWebMailer 7.21.0.01526 is susceptible to a remote code execution vulnerability in the Language parameter of mailingupgrade.php. An unauthenticated remote attacker can exploit this behavior to execute arbitrary PHP code via Code Injection.	9.8	More Details
CVE-2020-7593	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (V1.81.01 - V1.81.03), LOGO! 8 BM (incl. SIPLUS variants) (V1.82.01), LOGO! 8 BM (incl. SIPLUS variants) (V1.82.02). A buffer overflow vulnerability exists in the Web Server functionality of the device. A remote unauthenticated attacker could send a specially crafted HTTP request to cause a memory corruption, potentially resulting in remote code execution.	9.8	More Details
CVE-2020-1948	This vulnerability can affect all Dubbo users stay on version 2.7.6 or lower. An attacker can send RPC requests with unrecognized service name or method name along with some malicious parameter payloads. When the malicious parameter is deserialized, it will execute some malicious code. More details can be found below.	9.8	More Details
CVE-2020-11956	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a least privilege violation.	9.8	More Details
CVE-2020-11849	Elevation of privilege and/or unauthorized access vulnerability in Micro Focus Identity Manager. Affecting versions prior to 4.7.3 and 4.8.1 hot fix 1. The vulnerability could allow information exposure that can result in an elevation of privilege or an unauthorized access.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10038	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with access to the device's web server might be able to execute administrative commands without authentication.	9.8	More Details
CVE-2020-3931	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command.	9.8	More Details
CVE-2020-13926	Kylin concatenates and executes a Hive SQL in Hive CLI or beeline when building a new segment; some part of the HQL is from system configurations, while the configuration can be overwritten by certain rest api, which makes SQL injection attack is possible. Users of all previous versions after 2.0 should upgrade to 3.1.0.	9.8	More Details
CVE-2020-15504	A SQL injection vulnerability in the user and admin web interfaces of Sophos XG Firewall v18.0 MR1 and older potentially allows an attacker to run arbitrary code remotely. The fix is built into the re-release of XG Firewall v18 MR-1 (named MR-1-Build396) and the v17.5 MR13 release. All other versions >= 17.0 have received a hotfix.	9.8	More Details
CVE-2020-7458	In FreeBSD 12.1-STABLE before r362281, 11.4-STABLE before r362281, and 11.4-RELEASE before p1, long values in the user-controlled PATH environment variable cause posix_spawnp to write beyond the end of the heap allocated stack possibly leading to arbitrary code execution.	9.8	More Details
CVE-2020-13925	Similar to CVE-2020-1956, Kylin has one more restful API which concatenates the API inputs into OS commands and then executes them on the server; while the reported API misses necessary input validation, which causes the hackers to have the possibility to execute OS command remotely. Users of all previous versions after 2.3 should upgrade to 3.1.0.	9.8	More Details
CVE-2020-8186	A command injection vulnerability in the `devcert` module may lead to remote code execution when users of the module pass untrusted input to the `certificateFor` function.	9.8	More Details
CVE-2020-10042	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A buffer overflow in various positions of the web application might enable an attacker with access to the web application to execute arbitrary code over the network.	9.8	More Details
CVE-2020-10987	The goform/setUsbUnload endpoint of Tenda AC15 AC1900 version 15.03.05.19 allows remote attackers to execute arbitrary system commands via the deviceName POST parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10988	A hard-coded telnet credential in the tenda_login binary of Tenda AC15 AC1900 version 15.03.05.19 allows unauthenticated remote attackers to start a telnetd service on the device.	9.8	More Details
CVE-2020-11951	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a Backdoor root account.	9.8	More Details
CVE-2019-17638	In Eclipse Jetty, versions 9.4.27.v20200227 to 9.4.29.v20200521, in case of too large response headers, Jetty throws an exception to produce an HTTP 431 error. When this happens, the ByteBuffer containing the HTTP response headers is released back to the ByteBufferPool twice. Because of this double release, two threads can acquire the same ByteBuffer from the pool and while thread1 is about to use the ByteBuffer to write response1 data, thread2 fills the ByteBuffer with other data. Thread1 then proceeds to write the buffer that now contains different data. This results in client1, which issued request1 seeing data from another request or response which could contain sensitive data belonging to client2 (HTTP session ids, authentication credentials, etc.). If the Jetty version cannot be upgraded, the vulnerability can be significantly reduced by configuring a responseHeaderSize significantly larger than the requestHeaderSize (12KB responseHeaderSize and 8KB requestHeaderSize).	9.4	More Details
CVE-2020-11749	Pandora FMS 7.0 NG <= 746 suffers from Multiple XSS vulnerabilities in different browser views. A network administrator scanning a SNMP device can trigger a Cross Site Scripting (XSS), which can run arbitrary code to allow Remote Code Execution as root or apache2.	9.0	More Details
CVE-2020-1032	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043.	9.0	More Details
CVE-2020-1036	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1040	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043.	9.0	More Details
CVE-2020-1041	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1042, CVE-2020-1043.	9.0	More Details
CVE-2020-1042	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1043.	9.0	More Details
CVE-2020-1043	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-3973	The VeloCloud Orchestrator does not apply correct input validation which allows for blind SQL-injection. A malicious actor with tenant access to Velocloud Orchestrator could enter specially crafted SQL queries and obtain data to which they are not privileged.	8.8	More Details
CVE-2020-13994	An issue was discovered in Mods for HESK 3.1.0 through 2019.1.0. A privileged user can achieve code execution on the server via a ticket because of improper access control of uploaded resources. This might be exploitable in conjunction with CVE-2020-13992 by an unauthenticated attacker.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6289	SAP Disclosure Management, version 10.1, had insufficient protection against Cross-Site Request Forgery, which could be used to trick user in to browsing malicious site.	8.8	More Details
CVE-2020-15711	In MISP before 2.4.129, setting a favourite homepage was not CSRF protected.	8.8	More Details
CVE-2020-14300	The docker packages version docker-1.13.1-108.git4ef4b30.el7 as released for Red Hat Enterprise Linux 7 Extras via RHBA-2020:0053 (https://access.redhat.com/errata/RHBA-2020:0053) included an incorrect version of runc that was missing multiple bug and security fixes. One of the fixes regressed in that update was the fix for CVE-2016-9962, that was previously corrected in the docker packages in Red Hat Enterprise Linux 7 Extras via RHSA-2017:0116 (https://access.redhat.com/errata/RHSA-2017:0116). The CVE-2020-14300 was assigned to this security regression and it is specific to the docker packages produced by Red Hat. The original issue - CVE-2016-9962 - could possibly allow a process inside container to compromise a process entering container namespace and execute arbitrary code outside of the container. This could lead to compromise of the container host or other containers running on the same container host. This issue only affects a single version of Docker, 1.13.1-108.git4ef4b30, shipped in Red Hat Enterprise Linux 7. Both earlier and later versions are not affected.	8.8	More Details
CVE-2020-14298	The version of docker as released for Red Hat Enterprise Linux 7 Extras via RHBA-2020:0053 advisory included an incorrect version of runc missing the fix for CVE-2019-5736, which was previously fixed via RHSA-2019:0304. This issue could allow a malicious or compromised container to compromise the container host and other containers running on the same host. This issue only affects docker version 1.13.1-108.git4ef4b30.el7, shipped in Red Hat Enterprise Linux 7 Extras. Both earlier and later versions are not affected.	8.8	More Details
CVE-2020-8197	Privilege escalation vulnerability on Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows a low privileged user with management access to execute arbitrary commands.	8.8	More Details
CVE-2020-4305	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 could allow a remote attacker to execute arbitrary code on the system, caused by the deserialization of untrusted data. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 176677.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12426	Mozilla developers and community members reported memory safety bugs present in Firefox 77. 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 < 78.	8.8	More Details
CVE-2020-6292	Logout mechanism in SAP Disclosure Management, version 10.1, does not invalidate one of the session cookies, leading to Insufficient Session Expiration.	8.8	More Details
CVE-2020-12422	In non-standard configurations, a JPEG image created by JavaScript could have caused an internal variable to overflow, resulting in an out of bounds write, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 78.	8.8	More Details
CVE-2020-12420	When trying to connect to a STUN server, a race condition could have caused a use-after-free of a pointer, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.	8.8	More Details
CVE-2020-12419	When processing callbacks that occurred during window flushing in the parent process, the associated window may die; causing a use-after-free condition. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.	8.8	More Details
CVE-2020-12417	Due to confusion about ValueTags on JavaScript Objects, an object may pass through the type barrier, resulting in memory corruption and a potentially exploitable crash. *Note: this issue only affects Firefox on ARM64 platforms.* This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.	8.8	More Details
CVE-2020-12416	A VideoStreamEncoder may have been freed in a race condition with VideoBroadcaster::AddOrUpdateSink, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 78.	8.8	More Details
CVE-2020-12411	Mozilla developers reported memory safety bugs present in Firefox 76. 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 < 77.	8.8	More Details
CVE-2020-6291	SAP Disclosure Management, version 10.1, session mechanism does not have expiration data set therefore allows unlimited access after authenticating once, leading to Insufficient Session Expiration	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5764	MX Player Android App versions prior to v1.24.5, are vulnerable to a directory traversal vulnerability when user is using the MX Transfer feature in "Receive" mode. An attacker can exploit this by connecting to the MX Transfer session as a "sender" and sending a MessageType of "FILE_LIST" with a "name" field containing directory traversal characters (../). This will result in the file being transferred to the victim's phone, but being saved outside of the intended "/sdcard/MXshare" directory. In some instances, an attacker can achieve remote code execution by writing ".odex" and ".vdex" files in the "oat" directory of the MX Player application.	8.8	More Details
CVE-2020-12409	When using certain blank characters in a URL, they where incorrectly rendered as spaces instead of an encoded URL. This vulnerability affects Firefox < 77.	8.8	More Details
CVE-2020-1421	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-1448	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1447.	8.8	More Details
CVE-2020-1447	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1448.	8.8	More Details
CVE-2020-1446	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1447, CVE-2020-1448.	8.8	More Details
CVE-2020-1439	A remote code execution vulnerability exists in PerformancePoint Services for SharePoint Server when the software fails to check the source markup of XML file input, aka 'PerformancePoint Services Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-1436	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted fonts.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Windows Font Library Remote Code Execution Vulnerability'.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1435	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-1416	An elevation of privilege vulnerability exists in Visual Studio and Visual Studio Code when they load software dependencies, aka 'Visual Studio and Visual Studio Code Elevation of Privilege Vulnerability'.	8.8	More Details
CVE-2020-11953	An issue was discovered on Rittal PDU-3C002DEC through 5.15.40 and CMCIII-PU-9333E0FB through 3.15.70_4 devices. Attackers can execute code.	8.8	More Details
CVE-2020-1412	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-1408	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-1240	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-5374	Dell EMC OpenManage Integration for Microsoft System Center (OMIMSSC) for SCCM and SCVMM versions prior to 7.2.1 contain a hard-coded cryptographic key vulnerability. A remote unauthenticated attacker may exploit this vulnerability to gain access to the appliance data for remotely managed devices.	8.8	More Details
CVE-2019-12784	An issue was discovered in Verint Impact 360 15.1. At wfo/control/signin, the login form can accept submissions from external websites. In conjunction with CVE-2019-12783, this can be used by attackers to "crowdsource" bruteforce login attempts on the target site, allowing them to guess and potentially compromise valid credentials without ever sending any traffic from their own machine to the target site.	8.8	More Details
CVE-2020-11955	An issue was discovered on Rittal PDU-3C002DEC through 5.15.70 and CMCIII-PU-9333E0FB through 3.15.70 devices. There are insecure permissions.	8.8	More Details
CVE-2020-12410	Mozilla developers reported memory safety bugs present in Firefox 76 and Firefox ESR 68.8. 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 Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10045	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An error in the challenge-response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application.	8.8	More Details
CVE-2020-1481	A remote code execution vulnerability exists in the ESLint extension for Visual Studio Code when it validates source code after opening a project, aka 'Visual Studio Code ESLint Extention Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-12406	Mozilla Developer Iain Ireland discovered a missing type check during unboxed objects removal, resulting in a crash. We presume that with enough effort that it could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.	8.8	More Details
CVE-2020-15072	An issue was discovered in phpList through 3.5.4. An error-based SQL Injection vulnerability exists via the Import Administrators section.	8.8	More Details
CVE-2020-9377	D-Link DIR-610 devices allow Remote Command Execution via the cmd parameter to command.php. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	8.8	More Details
CVE-2018-12371	An integer overflow vulnerability in the Skia library when allocating memory for edge builders on some systems with at least 16 GB of RAM. This results in the use of uninitialized memory, resulting in a potentially exploitable crash. This vulnerability affects Firefox ESR < 60.1, Thunderbird < 60, and Firefox < 61.	8.8	More Details
CVE-2020-15093	The tough library (Rust/crates.io) prior to version 0.7.1 does not properly verify the threshold of cryptographic signatures. It allows an attacker to duplicate a valid signature in order to circumvent TUF requiring a minimum threshold of unique signatures before the metadata is considered valid. A fix is available in version 0.7.1. CVE-2020-6174 is assigned to the same vulnerability in the TUF reference implementation.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7587	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions < V3.3), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions < V2.6), SIMATIC IT Production Suite (All versions < V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions < V3.0 SP1), SIMATIC STEP 7 (TIA Portal) V15 (All versions < V15.1 Update 5), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES V15.1 (All versions < V15.1 Update 4), SIMOCODE ES V16 (All versions < V16 Update 1), Soft Starter ES V15.1 (All versions < V15.1 Update 3), Soft Starter ES V16 (All versions < V16 Update 1). Sending multiple specially crafted packets to the affected service could cause a partial remote denial-of-service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service.	8.2	More Details
CVE-2020-7578	A vulnerability has been identified in Camstar Enterprise Platform (All versions), Opcenter Execution Core (All versions < V8.2). Authenticated users could have access to resources they normally would not have. This vulnerability could allow an attacker to view internal information and perform unauthorized changes.	8.1	More Details
CVE-2020-7577	A vulnerability has been identified in Camstar Enterprise Platform (All versions), Opcenter Execution Core (All versions < V8.2). Through the use of several vulnerable fields of the application, an authenticated user could perform an SQL Injection attack by passing a modified SQL query downstream to the back-end server. The exploit of this vulnerability could be used to read, and potentially modify application data to which the user has access to.	8.1	More Details
CVE-2020-7457	In FreeBSD 12.1-STABLE before r359565, 12.1-RELEASE before p7, 11.4-STABLE before r362975, 11.4-RELEASE before p1, and 11.3-RELEASE before p11, missing synchronization in the IPV6_2292PKTOPTIONS socket option set handler contained a race condition allowing a malicious application to modify memory after being freed, possibly resulting in code execution.	8.1	More Details
CVE-2020-5604	Android App 'Mercari' (Japan version) prior to version 3.52.0 allows arbitrary method execution of a Java object by a remote attacker via a Man-In-The-Middle attack by using Java Reflection API of JavaScript code on WebView.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2034	An OS Command Injection vulnerability in the PAN-OS GlobalProtect portal allows an unauthenticated network based attacker to execute arbitrary OS commands with root privileges. An attacker requires some knowledge of the firewall to exploit this issue. This issue can not be exploited if GlobalProtect portal feature is not enabled. This issue impacts PAN-OS 9.1 versions earlier than PAN-OS 9.1.3; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; all versions of PAN-OS 8.0 and PAN-OS 7.1. Prisma Access services are not impacted by this vulnerability.	8.1	More Details
CVE-2020-10039	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker in a privileged network position between a legitimate user and the web server might be able to conduct a Man-in-the-middle attack and gain read and write access to the transmitted data.	8.1	More Details
CVE-2020-1370	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422.	7.8	More Details
CVE-2020-1372	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles objects in memory, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1405.	7.8	More Details
CVE-2020-1371	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1365.	7.8	More Details
CVE-2019-4591	IBM Maximo Asset Management 7.6.0 and 7.6.1 does not invalidate session after logout which could allow a local user to impersonate another user on the system. IBM X-Force ID: 167451.	7.8	More Details
CVE-2020-1369	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1344, CVE-2020-1362.	7.8	More Details
CVE-2020-1368	An elevation of privilege vulnerability exists in the way that the Credential Enrollment Manager service handles objects in memory, aka 'Windows Credential Enrollment Manager Service Elevation of Privilege Vulnerability'.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1375	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1373	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1390, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438.	7.8	More Details
CVE-2020-1388	An elevation of privilege vulnerability exists in the way that the psmsrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1392, CVE-2020-1394, CVE-2020-1395.	7.8	More Details
CVE-2020-8199	Improper access control in Citrix ADC Gateway Linux client versions before 1.0.0.137 results in local privilege escalation to root.	7.8	More Details
CVE-2020-1381	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1382.	7.8	More Details
CVE-2020-1384	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1359.	7.8	More Details
CVE-2020-1385	An elevation of privilege vulnerability exists in the way that the Windows Credential Picker handles objects in memory, aka 'Windows Credential Picker Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1387	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notification Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1365	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1371.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1390	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438.	7.8	More Details
CVE-2020-1392	An elevation of privilege vulnerability exists when the Windows Delivery Optimization service improperly handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1394, CVE-2020-1395.	7.8	More Details
CVE-2020-1393	An elevation of privilege vulnerability exists when the Windows Diagnostics Hub Standard Collector Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka 'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1418.	7.8	More Details
CVE-2020-1394	An elevation of privilege vulnerability exists in the way that the Windows Geolocation Framework handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1392, CVE-2020-1395.	7.8	More Details
CVE-2020-1366	An elevation of privilege vulnerability exists when the Windows Print Workflow Service improperly handles objects in memory, aka 'Windows Print Workflow Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1359	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1384.	7.8	More Details
CVE-2020-1363	An elevation of privilege vulnerability exists when the Windows Picker Platform improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Picker Platform Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1362	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1344, CVE-2020-1369.	7.8	More Details
CVE-2020-5974	NVIDIA JetPack SDK, version 4.2 and 4.3, contains a vulnerability in its installation scripts in which permissions are incorrectly set on certain directories, which can lead to escalation of privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1085	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1147	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-1249	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422.	7.8	More Details
CVE-2020-1336	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Kernel properly handles objects in memory.	7.8	More Details
CVE-2020-1344	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1362, CVE-2020-1369.	7.8	More Details
CVE-2020-1346	An elevation of privilege vulnerability exists when the Windows Modules Installer improperly handles file operations, aka 'Windows Modules Installer Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1347	An elevation of privilege vulnerability exists when the Windows Storage Services improperly handle file operations, aka 'Windows Storage Services Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1349	A remote code execution vulnerability exists in Microsoft Outlook software when it fails to properly handle objects in memory, aka 'Microsoft Outlook Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-1352	An elevation of privilege vulnerability exists when the Windows USO Core Worker improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows USO Core Worker Elevation of Privilege Vulnerability'.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1353	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422.	7.8	More Details
CVE-2020-1354	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1430.	7.8	More Details
CVE-2020-1355	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-1356	An elevation of privilege vulnerability exists when the Windows iSCSI Target Service improperly handles file operations, aka 'Windows iSCSI Target Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1357	An elevation of privilege vulnerability exists when the Windows System Events Broker improperly handles file operations, aka 'Windows System Events Broker Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1396	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1360	An elevation of privilege vulnerability exists when the Windows Profile Service improperly handles file operations, aka 'Windows Profile Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1395	An elevation of privilege vulnerability exists in the way that the Windows Speech Brokered API handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1392, CVE-2020-1394.	7.8	More Details
CVE-2020-1382	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1381.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1424	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka 'Windows Update Stack Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1413	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422.	7.8	More Details
CVE-2020-1415	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1422.	7.8	More Details
CVE-2020-1418	An elevation of privilege vulnerability exists when the Windows Diagnostics Execution Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka 'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1393.	7.8	More Details
CVE-2020-7815	XPLATFORM v9.2.260 and eariler versions contain a vulnerability that could allow remote files to be downloaded by setting the arguments to the vulnerable method. this can be leveraged for code execution. File download vulnerability in ____COMPONENT____ of TOBESOFT XPLATFORM allows ____ATTACKER/ATTACK____ to cause ____IMPACT____. This issue affects: TOBESOFT XPLATFORM 9.2.250 versions prior to 9.2.260 on Windows.	7.8	More Details
CVE-2020-3974	VMware Fusion (11.x before 11.5.5), VMware Remote Console for Mac (11.x and prior before 11.2.0) and Horizon Client for Mac (5.x and prior before 5.4.3) contain a privilege escalation vulnerability due to improper XPC Client validation. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMware Remote Console for Mac or Horizon Client for Mac is installed.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7814	RAONWIZ v2018.0.2.50 and eariler versions contains a vulnerability that could allow remote files to be downloaded and excuted by lack of validation to file extension, witch can used as remote-code-excution attacks by hackers File download & execution vulnerability in ____COMPONENT____ of RAONWIZ RAON KUpload allows ____ATTACKER/ATTACK____ to cause ____IMPACT____. This issue affects: RAONWIZ RAON KUpload 2018.0.2.50 versions prior to 2018.0.2.51 on Windows.	7.8	More Details
CVE-2020-1422	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415.	7.8	More Details
CVE-2020-1423	An elevation of privilege vulnerability exists in the way that the Windows Subsystem for Linux handles files, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1427	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1428, CVE-2020-1438.	7.8	More Details
CVE-2020-1428	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1438.	7.8	More Details
CVE-2020-1429	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1430	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1354.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1431	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1437	An elevation of privilege vulnerability exists in the way that the Windows Network Location Awareness Service handles objects in memory, aka 'Windows Network Location Awareness Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1438	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1428.	7.8	More Details
CVE-2020-12423	When the Windows DLL "webauthn.dll" was missing from the Operating System, and a malicious one was placed in a folder in the user's %PATH%, Firefox may have loaded the DLL, leading to arbitrary code execution. *Note: This issue only affects the Windows operating system; other operating systems are unaffected.* This vulnerability affects Firefox < 78.	7.8	More Details
CVE-2020-1449	A remote code execution vulnerability exists in Microsoft Project software when the software fails to check the source markup of a file, aka 'Microsoft Project Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-1458	A remote code execution vulnerability exists when Microsoft Office improperly validates input before loading dynamic link library (DLL) files, aka 'Microsoft Office Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-1463	An elevation of privilege vulnerability exists in the way that the SharedStream Library handles objects in memory, aka 'Windows SharedStream Library Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1465	An elevation of privilege vulnerability exists in Microsoft OneDrive that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft OneDrive Elevation of Privilege Vulnerability'.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1414	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1415, CVE-2020-1422.	7.8	More Details
CVE-2020-11827	In GOG Galaxy 1.2.67, there is a service that is vulnerable to weak file/service permissions: GalaxyClientService.exe. An attacker can put malicious code in a Trojan horse GalaxyClientService.exe. After that, the attacker can re-start this service as an unprivileged user to escalate his/her privileges and run commands on the machine with SYSTEM rights.	7.8	More Details
CVE-2020-1411	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1336.	7.8	More Details
CVE-2020-1399	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422.	7.8	More Details
CVE-2020-1404	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422.	7.8	More Details
CVE-2020-1410	A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vcard files.To exploit the vulnerability, an attacker could send a malicious vcard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-1400	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1401, CVE-2020-1407.	7.8	More Details
CVE-2020-1401	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1400, CVE-2020-1407.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1409	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'.	7.8	More Details
CVE-2020-1402	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1406	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-1407	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1400, CVE-2020-1401.	7.8	More Details
CVE-2020-5246	Traccar GPS Tracking System before version 4.9 has a LDAP injection vulnerability. It occurs when user input is being used in LDAP search filter. By providing specially crafted input, an attacker can modify the logic of the LDAP query and get admin privileges. The issue only impacts instances with LDAP configuration and where users can craft their own names. This has been patched in version 4.9.	7.7	More Details
CVE-2020-9376	D-Link DIR-610 devices allow Information Disclosure via SERVICES=DEVICE.ACCOUNT%0AAUTHORIZED_GROUP=1 to getcfg.php. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.5	More Details
CVE-2020-8190	Incorrect file permissions in Citrix ADC and Citrix Gateway before versions 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows privilege escalation.	7.5	More Details
CVE-2020-8187	Improper input validation in Citrix ADC and Citrix Gateway versions before 11.1-63.9 and 12.0-62.10 allows unauthenticated users to perform a denial of service attack.	7.5	More Details
CVE-2020-1403	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'.	7.5	More Details
CVE-2020-12398	If Thunderbird is configured to use STARTTLS for an IMAP server, and the server sends a PREAUTH response, then Thunderbird will continue with an unencrypted connection, causing email data to be sent without protection. This vulnerability affects Thunderbird < 68.9.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20898	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to access sensitive information without being authenticated in the Global permissions screen. The affected versions are before version 8.8.0.	7.5	More Details
CVE-2020-10037	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information.	7.5	More Details
CVE-2020-5839	Symantec Endpoint Detection And Response, prior to 4.4, may be susceptible to an information disclosure issue, which is a type of vulnerability that could potentially allow unauthorized access to data.	7.5	More Details
CVE-2020-11994	Server-Side Template Injection and arbitrary file disclosure on Camel templating components	7.5	More Details
CVE-2020-13993	An issue was discovered in Mods for HESK 3.1.0 through 2019.1.0. A blind time-based SQL injection issue allows remote unauthenticated attackers to retrieve information from the database via a ticket.	7.5	More Details
CVE-2020-10044	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with access to the network could be able to install specially crafted firmware to the device.	7.5	More Details
CVE-2020-13934	An h2c direct connection to Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M5 to 9.0.36 and 8.5.1 to 8.5.56 did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of service.	7.5	More Details
CVE-2020-15074	OpenVPN Access Server older than version 2.8.4 and version 2.9.5 generates new user authentication tokens instead of reusing exiting tokens on reconnect making it possible to circumvent the initial token expiry timestamp.	7.5	More Details
CVE-2020-13846	Sylabs Singularity 3.5.0 through 3.5.3 fails to report an error in a Status Code.	7.5	More Details
CVE-2020-13847	Sylabs Singularity 3.0 through 3.5 lacks support for an Integrity Check. Singularity's sign and verify commands do not sign metadata found in the global header or data object descriptors of a SIF file.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6938	A sensitive information disclosure vulnerability in Tableau Server 10.5, 2018.x, 2019.x, 2020.x released before June 26, 2020, could allow access to sensitive information in log files.	7.5	More Details
CVE-2019-19415	The SIP module of some Huawei products have a denial of service (DoS) vulnerability. A remote attacker could exploit these three vulnerabilities by sending the specially crafted messages to the affected device. Due to the insufficient verification of the packets, successful exploit could allow the attacker to cause buffer overflow and dead loop, leading to DoS condition. Affected products can be found in https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200115-01-sip-en.	7.5	More Details
CVE-2019-19416	The SIP module of some Huawei products have a denial of service (DoS) vulnerability. A remote attacker could exploit these three vulnerabilities by sending the specially crafted messages to the affected device. Due to the insufficient verification of the packets, successful exploit could allow the attacker to cause buffer overflow and dead loop, leading to DoS condition. Affected products can be found in https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200115-01-sip-en.	7.5	More Details
CVE-2020-15050	An issue was discovered in the Video Extension in Suprema BioStar 2 before 2.8.2. Remote attackers can read arbitrary files from the server via Directory Traversal.	7.5	More Details
CVE-2019-19417	The SIP module of some Huawei products have a denial of service (DoS) vulnerability. A remote attacker could exploit these three vulnerabilities by sending the specially crafted messages to the affected device. Due to the insufficient verification of the packets, successful exploit could allow the attacker to cause buffer overflow and dead loop, leading to DoS condition. Affected products can be found in https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200115-01-sip-en.	7.5	More Details
CVE-2020-1374	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.	7.5	More Details
CVE-2019-20907	In Lib/tarfile.py in Python through 3.8.3, an attacker is able to craft a TAR archive leading to an infinite loop when opened by tarfile.open, because _proc_pax lacks header validation.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15689	Appweb before 7.2.2 and 8.x before 8.1.0, when built with CGI support, mishandles an HTTP request with a Range header that lacks an exact range. This may result in a NULL pointer dereference and cause a denial of service.	7.5	More Details
CVE-2020-5766	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in SRS Simple Hits Counter Plugin for WordPress 1.0.3 and 1.0.4 allows a remote, unauthenticated attacker to determine the value of database fields.	7.5	More Details
CVE-2020-1469	A denial of service vulnerability exists when the .NET implementation of Bond improperly parses input, aka 'Bond Denial of Service Vulnerability'.	7.5	More Details
CVE-2020-7584	A vulnerability has been identified in SIMATIC S7-200 SMART CPU family (All versions >= V2.2 < V2.5.1). Affected devices do not properly handle large numbers of new incomming connections and could crash under certain circumstances. An attacker may leverage this to cause a Denial-of-Service situation.	7.5	More Details
CVE-2020-13845	Sylabs Singularity 3.0 through 3.5 has Improper Validation of an Integrity Check Value. Image integrity is not validated when an ECL policy is enforced. The fingerprint required by the ECL is compared against the signature object descriptor(s) in the SIF file, rather than to a cryptographically validated signature.	7.5	More Details
CVE-2020-13935	The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.	7.5	More Details
CVE-2020-7692	PKCE support is not implemented in accordance with the RFC for OAuth 2.0 for Native Apps. Without the use of PKCE, the authorization code returned by an authorization server is not enough to guarantee that the client that issued the initial authorization request is the one that will be authorized. An attacker is able to obtain the authorization code using a malicious app on the client-side and use it to gain authorization to the protected resource. This affects the package com.google.oauth-client:google-oauth-client before 1.31.0.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2030	An OS Command Injection vulnerability in the PAN-OS management interface that allows authenticated administrators to execute arbitrary OS commands with root privileges. This issue impacts PAN-OS 8.1 versions earlier than PAN-OS 8.1.15; and all versions of PAN-OS 7.1 and PAN-OS 8.0. This issue does not impact PAN-OS 9.0, PAN-OS 9.1, or Prisma Access services.	7.2	More Details
CVE-2020-15092	In TimelineJS before version 3.7.0, some user data renders as HTML. An attacker could implement an XSS exploit with maliciously crafted content in a number of data fields. This risk is present whether the source data for the timeline is stored on Google Sheets or in a JSON configuration file. Most TimelineJS users configure their timeline with a Google Sheets document. Those users are exposed to this vulnerability if they grant write access to the document to a malicious inside attacker, if the access of a trusted user is compromised, or if they grant public write access to the document. Some TimelineJS users configure their timeline with a JSON document. Those users are exposed to this vulnerability if they grant write access to the document to a malicious inside attacker, if the access of a trusted user is compromised, or if write access to the system hosting that document is otherwise compromised. Version 3.7.0 of TimelineJS addresses this in two ways. For content which is intended to support limited HTML markup for styling and linking, that content is "sanitized" before being added to the DOM. For content intended for simple text display, all markup is stripped. Very few users of TimelineJS actually install the TimelineJS code on their server. Most users publish a timeline using a URL hosted on systems we control. The fix for this issue is published to our system such that **those users will automatically begin using the new code**. The only exception would be users who have deliberately edited the embed URL to "pin" their timeline to an earlier version of the code. Some users of TimelineJS use it as a part of a wordpress plugin (knight-lab-timelinejs). Version 3.7.0.0 of that plugin and newer integrate the updated code. Users are encouraged to update the plugin rather than manually update the embedded version of TimelineJS.	7.2	More Details
CVE-2020-6114	An exploitable SQL injection vulnerability exists in the Admin Reports functionality of Glacies IceHRM v26.6.0.OS (Commit bb274de1751ffb9d09482fd2538f9950a94c510a) . A specially crafted HTTP request can cause SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	7.2	More Details
CVE-2020-4512	IBM QRadar SIEM 7.3 and 7.4 could allow a remote privileged user to execute commands.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5366	Dell EMC iDRAC9 versions prior to 4.20.20.20 contain a Path Traversal Vulnerability. A remote authenticated malicious user with low privileges could potentially exploit this vulnerability by manipulating input parameters to gain unauthorized read access to the arbitrary files.	7.1	More Details
CVE-2020-1364	A denial of service vulnerability exists in the way that the WalletService handles files, aka 'Windows WalletService Denial of Service Vulnerability'.	7.1	More Details
CVE-2020-1461	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'.	7.1	More Details
CVE-2020-1405	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1372.	7.1	More Details
CVE-2020-1398	An elevation of privilege vulnerability exists when Windows Lockscreen fails to properly handle Ease of Access dialog.An attacker who successfully exploited the vulnerability could execute commands with elevated permissions.The security update addresses the vulnerability by ensuring that the Ease of Access dialog is handled properly., aka 'Windows Lockscreen Elevation of Privilege Vulnerability'.	6.8	More Details
CVE-2020-15720	In Dogtag PKI through 10.8.3, the pki.client.PKIConnection class did not enable python-requests certificate validation. Since the verify parameter was hard-coded in all request functions, it was not possible to override the setting. As a result, tools making use of this class, such as the pki-server command, may have been vulnerable to Person-in-the-Middle attacks in certain non-localhost use cases. This is fixed in 10.9.0-b1.	6.8	More Details
CVE-2020-4042	Bareos before version 19.2.8 and earlier allows a malicious client to communicate with the director without knowledge of the shared secret if the director allows client initiated connection and connects to the client itself. The malicious client can replay the Bareos director's cram-md5 challenge to the director itself leading to the director responding to the replayed challenge. The response obtained is then a valid reply to the directors original challenge. This is fixed in version 19.2.8.	6.8	More Details
CVE-2020-1333	An elevation of privilege vulnerability exists when Group Policy Services Policy Processing improperly handle reparse points, aka 'Group Policy Services Policy Processing Elevation of Privilege Vulnerability'.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7581	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions < V3.3), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions < V3.0 SP1), SIMATIC STEP 7 (TIA Portal) V15 (All versions < V15.1 Update 5), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES V15.1 (All versions < V15.1 Update 4), SIMOCODE ES V16 (All versions < V16 Update 1), Soft Starter ES V15.1 (All versions < V15.1 Update 3), Soft Starter ES V16 (All versions < V16 Update 1). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. This could allow a local attacker with administrative privileges to execute code with SYSTEM level privileges.	6.7	More Details
CVE-2020-1468	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'.	6.5	More Details
CVE-2020-5373	Dell EMC OpenManage Integration for Microsoft System Center (OMIMSSC) for SCCM and SCVMM versions prior to 7.2.1 contain an improper authentication vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to retrieve the system inventory data of the managed device.	6.5	More Details
CVE-2020-1433	An information disclosure vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Information Disclosure Vulnerability'.	6.5	More Details
CVE-2020-12407	Mozilla Developer Nicolas Silva found that when using WebRender, Firefox would under certain conditions leak arbitrary GPU memory to the visible screen. The leaked memory content was visible to the user, but not observable from web content. This vulnerability affects Firefox < 77.	6.5	More Details
CVE-2020-1397	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows Imaging Component Information Disclosure Vulnerability'.	6.5	More Details
CVE-2020-12408	When browsing a document hosted on an IP address, an attacker could insert certain characters to flip domain and path information in the address bar. This vulnerability affects Firefox < 77.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12424	When constructing a permission prompt for WebRTC, a URI was supplied from the content process. This URI was untrusted, and could have been the URI of an origin that was previously granted permission; bypassing the prompt. This vulnerability affects Firefox < 78.	6.5	More Details
CVE-2020-4511	IBM QRadar SIEM 7.3 and 7.4 could allow an authenticated user to cause a denial of service of the qflow process by sending a malformed sflow command. IBM X-Force ID: 182366.	6.5	More Details
CVE-2020-8193	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints.	6.5	More Details
CVE-2020-12421	When performing add-on updates, certificate chains terminating in non-built-in-roots were rejected (even if they were legitimately added by an administrator.) This could have caused add-ons to become out-of-date silently without notification to the user. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.	6.5	More Details
CVE-2020-12425	Due to confusion processing a hyphen character in Date.parse(), a one-byte out of bounds read could have occurred, leading to potential information disclosure. This vulnerability affects Firefox < 78.	6.5	More Details
CVE-2020-8194	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download.	6.5	More Details
CVE-2020-10756	An out-of-bounds read vulnerability was found in the SLiRP networking implementation of the QEMU emulator. This flaw occurs in the icmp6_send_echoreply() routine while replying to an ICMP echo request, also known as ping. This flaw allows a malicious guest to leak the contents of the host memory, resulting in possible information disclosure. This flaw affects versions of libslirp before 4.3.1.	6.5	More Details
CVE-2020-8195	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users.	6.5	More Details
CVE-2020-14171	Atlassian Bitbucket Server from version 4.9.0 before version 7.2.4 allows remote attackers to intercept unencrypted repository import requests via a Man-in-the-Middle (MITM) attack.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9260	HUAWEI P30 and HUAWEI P30 Pro smartphones with versions earlier than 10.1.0.123(C432E22R2P5) and versions earlier than 10.1.0.160(C00E160R2P8) have an information disclosure vulnerability. Certain WI-FI function's default configuration in the system seems insecure, an attacker should craft a WI-FI hotspot to launch the attack. Successful exploit could cause information disclosure.	6.5	More Details
CVE-2019-20897	The avatar upload feature in affected versions of Atlassian Jira Server and Data Center allows remote attackers to achieve Denial of Service via a crafted PNG file. The affected versions are before version 8.5.4, from version 8.6.0 before 8.6.2, and from version 8.7.0 before 8.7.1.	6.5	More Details
CVE-2020-7592	A vulnerability has been identified in SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI KTP700F Mobile Arctic (All versions), SIMATIC HMI Mobile Panels 2nd Generation (All versions), SIMATIC WinCC Runtime Advanced (All versions). Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information.	6.5	More Details
CVE-2020-10986	A CSRF issue in the /goform/SysToolReboot endpoint of Tenda AC15 AC1900 version 15.03.05.19 allows remote attackers to reboot the device and cause denial of service via a payload hosted by an attacker-controlled web page.	6.5	More Details
CVE-2020-12415	When "%2F" was present in a manifest URL, Firefox's AppCache behavior may have become confused and allowed a manifest to be served from a subdirectory. This could cause the appcache to be used to service requests for the top level directory. This vulnerability affects Firefox < 78.	6.5	More Details
CVE-2020-12414	IndexedDB should be cleared when leaving private browsing mode and it is not, the API for WKWebViewConfiguration was being used incorrectly and requires the private instance of this object be deleted when leaving private mode. This vulnerability affects Firefox for iOS < 27.	6.5	More Details
CVE-2020-12418	Manipulating individual parts of a URL object could have caused an out-of-bounds read, leaking process memory to malicious JavaScript. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6285	SAP NetWeaver - XML Toolkit for JAVA (ENGINEAPI) (versions- 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50), under certain conditions allows an attacker to access information which would otherwise be restricted, leading to Information Disclosure.	6.5	More Details
CVE-2020-11084	In iPear, the manual execution of the eval() function can lead to command injection. Only PCs where commands are manually executed via "For Developers" are affected. This function allows executing any PHP code within iPear which may change, damage, or steal data (files) from the PC.	6.4	More Details
CVE-2020-6290	SAP Disclosure Management, version 10.1, is vulnerable to Session Fixation attacks wherein the attacker tricks the user into using a specific session ID.	6.3	More Details
CVE-2020-11952	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. Attackers can bypass the CLI menu.	6.2	More Details
CVE-2020-4513	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 182368.	6.1	More Details
CVE-2020-8198	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS).	6.1	More Details
CVE-2020-8191	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS).	6.1	More Details
CVE-2019-20901	The login.jsp resource in Jira before version 8.5.2, and from version 8.6.0 before version 8.6.1 allows remote attackers to redirect users to a different website which they may use as part of performing a phishing attack via an open redirect in the os_destination parameter.	6.1	More Details
CVE-2020-6276	SAP Business Objects Business Intelligence Platform (bipodata), version 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting vulnerability.	6.1	More Details
CVE-2020-6281	SAP Business Objects Business Intelligence Platform (BI Launchpad), version 4.2, does not sufficiently encode user-controlled inputs, resulting reflected in Cross-Site Scripting.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1442	A spoofing vulnerability exists when an Office Web Apps server does not properly sanitize a specially crafted request, aka 'Office Web Apps XSS Vulnerability'.	6.1	More Details
CVE-2019-12773	An issue was discovered in Verint Impact 360 15.1. At wfo/help/help_popup.jsp, the helpURL parameter can be changed to embed arbitrary content inside of an iFrame. Attackers may use this in conjunction with social engineering to embed malicious scripts or phishing pages on a site where this product is installed, given the attacker can convince a victim to visit a crafted link.	6.1	More Details
CVE-2020-15299	A reflected Cross-Site Scripting (XSS) Vulnerability in the KingComposer plugin through 2.9.4 for WordPress allows remote attackers to trick a victim into submitting an install_online_preset AJAX request containing base64-encoded JavaScript (in the kc-online-preset-data POST parameter) that is executed in the victim's browser.	6.1	More Details
CVE-2020-10989	An XSS issue in the /goform/WifiBasicSet endpoint of Tenda AC15 AC1900 version 15.03.05.19 allows remote attackers to execute malicious payloads via the WifiName POST parameter.	6.1	More Details
CVE-2020-13992	An issue was discovered in Mods for HESK 3.1.0 through 2019.1.0. A Stored XSS issue allows remote unauthenticated attackers to abuse a helpdesk user's logged in session. A user with sufficient privileges to change their login-page image must open a crafted ticket.	6.1	More Details
CVE-2020-5607	Open redirect vulnerability in SHIRASAGI v1.13.1 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	6.1	More Details
CVE-2020-10041	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A stored Cross-Site-Scripting (XSS) vulnerability is present in different locations of the web application. An attacker might be able to take over a session of a legitimate user.	6.1	More Details
CVE-2020-10043	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12783	An issue was discovered in Verint Impact 360 15.1. At wfo/control/signin, the rd parameter can accept a URL, to which users will be redirected after a successful login. In conjunction with CVE-2019-12784, this can be used by attackers to "crowdsource" bruteforce login attempts on the target site, allowing them to guess and potentially compromise valid credentials without ever sending any traffic from their own machine to the target site.	6.1	More Details
CVE-2020-7140	A security vulnerability in HPE IceWall SSO Dfw and Dgfw (Domain Gateway Option) could be exploited remotely to cause a remote cross-site scripting (XSS). HPE has provided the following information to resolve this vulnerability in HPE IceWall SSO DFW and Dgfw: https://www.hpe.com/jp/icewall_patchaccess	6.1	More Details
CVE-2020-15721	RosarioSIS through 6.8-beta allows modules/Custom/NotifyParents.php XSS because of the href attributes for AddStudents.php and User.php.	6.1	More Details
CVE-2020-11061	In Bareos Director less than or equal to 16.2.10, 17.2.9, 18.2.8, and 19.2.7, a heap overflow allows a malicious client to corrupt the director's memory via oversized digest strings sent during initialization of a verify job. Disabling verify jobs mitigates the problem. This issue is also patched in Bareos versions 19.2.8, 18.2.9 and 17.2.10.	6.0	More Details
CVE-2020-15000	A PIN management problem was discovered on Yubico YubiKey 5 devices 5.2.0 to 5.2.6. OpenPGP has three passwords: Admin PIN, Reset Code, and User PIN. The Reset Code is used to reset the User PIN, but it is disabled by default. A flaw in the implementation of OpenPGP sets the Reset Code to a known value upon initialization. If the retry counter for the Reset Code is set to non-zero without changing the Reset Code, this known value can be used to reset the User PIN. To set the retry counters, the Admin PIN is required.	5.9	More Details
CVE-2020-15526	In Redgate SQL Monitor 7.1.4 through 10.1.6 (inclusive), the scope for disabling some TLS security certificate checks can extend beyond that defined by various options on the Configuration > Notifications pages to disable certificate checking for alert notifications. These TLS security checks are also ignored during monitoring of VMware machines. This would make SQL Monitor vulnerable to potential man-in-the-middle attacks when sending alert notification emails, posting to Slack or posting to webhooks. The vulnerability is fixed in version 10.1.7.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6282	SAP NetWeaver AS JAVA (IIOP service) (SERVERCORE), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, and SAP NetWeaver AS JAVA (IIOP service) (CORE-TOOLS), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker to send a crafted request from a vulnerable web application. It is usually used to target internal systems behind firewalls that are normally inaccessible to an attacker from the external network, resulting in a Server-Side Request Forgery vulnerability.	5.8	More Details
CVE-2020-1420	An information disclosure vulnerability exists when Windows Error Reporting improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Error Reporting Information Disclosure Vulnerability'.	5.5	More Details
CVE-2019-19338	A flaw was found in the fix for CVE-2019-11135, in the Linux upstream kernel versions before 5.5 where, the way Intel CPUs handle speculative execution of instructions when a TSX Asynchronous Abort (TAA) error occurs. When a guest is running on a host CPU affected by the TAA flaw (TAA_NO=0), but is not affected by the MDS issue (MDS_NO=1), the guest was to clear the affected buffers by using a VERW instruction mechanism. But when the MDS_NO=1 bit was exported to the guests, the guests did not use the VERW mechanism to clear the affected buffers. This issue affects guests running on Cascade Lake CPUs and requires that host has 'TSX' enabled. Confidentiality of data is the highest threat associated with this vulnerability.	5.5	More Details
CVE-2020-1391	An information disclosure vulnerability exists when the Windows Agent Activation Runtime (AarSvc) fails to properly handle objects in memory, aka 'Windows Agent Activation Runtime Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-1419	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1426.	5.5	More Details
CVE-2020-9258	HUAWEI P30 smartphone with versions earlier than 10.1.0.135(C00E135R2P11) have an improper input verification vulnerability. An attribution in a module is not set correctly and some verification is lacked. Attackers with local access can exploit this vulnerability by injecting malicious fragment. This may lead to user information leak.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1386	An information vulnerability exists when Windows Connected User Experiences and Telemetry Service improperly discloses file information, aka 'Connected User Experiences and Telemetry Service Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-1445	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1342.	5.5	More Details
CVE-2020-1389	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1419, CVE-2020-1426.	5.5	More Details
CVE-2020-1367	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1389, CVE-2020-1419, CVE-2020-1426.	5.5	More Details
CVE-2020-1361	An information disclosure vulnerability exists in the way that the WalletService handles memory.To exploit the vulnerability, an attacker would first need code execution on a victim system, aka 'Windows WalletService Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-4510	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 182365.	5.5	More Details
CVE-2020-10040	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with local access to the device might be able to retrieve some passwords in clear text.	5.5	More Details
CVE-2020-1330	An information disclosure vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-1342	An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1445.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1351	An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-1426	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1419.	5.5	More Details
CVE-2020-1358	An information disclosure vulnerability exists when the Windows Resource Policy component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Resource Policy Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-4364	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178961.	5.4	More Details
CVE-2020-1456	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1450, CVE-2020-1451.	5.4	More Details
CVE-2020-7576	A vulnerability has been identified in Camstar Enterprise Platform (All versions), Opcenter Execution Core (All versions < V8.2), Opcenter Execution Core (V8.2). An authenticated user with the ability to create containers, packages or register defects could perform stored Cross-Site Scripting (XSS) attacks within the vulnerable software. The impact of this attack could result in the session cookies of legitimate users being stolen. Should the attacker gain access to these cookies, they could then hijack the session and perform arbitrary actions in the name of the victim.	5.4	More Details
CVE-2020-15073	An issue was discovered in phpList through 3.5.4. An XSS vulnerability occurs within the Import Administrators section via upload of an edited text document. This also affects the Subscriber Lists section.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15105	Django Two-Factor Authentication before 1.12, stores the user's password in clear text in the user session (base64-encoded). The password is stored in the session when the user submits their username and password, and is removed once they complete authentication by entering a two-factor authentication code. This means that the password is stored in clear text in the session for an arbitrary amount of time, and potentially forever if the user begins the login process by entering their username and password and then leaves before entering their two-factor authentication code. The severity of this issue depends on which type of session storage you have configured: in the worst case, if you're using Django's default database session storage, then users' passwords are stored in clear text in your database. In the best case, if you're using Django's signed cookie session, then users' passwords are only stored in clear text within their browser's cookie store. In the common case of using Django's cache session store, the users' passwords are stored in clear text in whatever cache storage you have configured (typically Memcached or Redis). This has been fixed in 1.12. After upgrading, users should be sure to delete any clear text passwords that have been stored. For example, if you're using the database session backend, you'll likely want to delete any session record from the database and purge that data from any database backups or replicas. In addition, affected organizations who have suffered a database breach while using an affected version should inform their users that their clear text passwords have been compromised. All organizations should encourage users whose passwords were insecurely stored to change these passwords on any sites where they were used. As a workaround, wwitching Django's session storage to use signed cookies instead of the database or cache lessens the impact of this issue, but should not be done without a thorough understanding of the security tradeoffs of using signed cookies rather than a server-side session storage. There is no way to fully mitigate the issue without upgrading.	5.4	More Details
CVE-2020-1450	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1451, CVE-2020-1456.	5.4	More Details
CVE-2020-1451	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1450, CVE-2020-1456.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1454	This vulnerability is caused when SharePoint Server does not properly sanitize a specially crafted request to an affected SharePoint server.An authenticated attacker could exploit this vulnerability by sending a specially crafted request to an affected SharePoint server, aka 'Microsoft SharePoint Reflective XSS Vulnerability'.	5.4	More Details
CVE-2020-1326	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server does not properly sanitize user provided input, aka 'Azure DevOps Server Cross-site Scripting Vulnerability'.	5.4	More Details
CVE-2020-1443	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'.	5.4	More Details
CVE-2020-6278	SAP Business Objects Business Intelligence Platform (BI Launchpad and CMC), versions 4.1, 4.2, allows to an attacker to embed malicious scripts in the application while uploading images, which gets executed when the victim opens these files, leading to Stored Cross Site Scripting	5.4	More Details
CVE-2020-6267	Some sensitive cookies in SAP Disclosure Management, version 10.1, are missing HttpOnly flag, leading to sensitive cookie without Http Only flag.	5.4	More Details
CVE-2020-7693	Incorrect handling of Upgrade header with the value websocket leads in crashing of containers hosting sockjs apps. This affects the package sockjs before 0.3.20.	5.3	More Details
CVE-2020-15001	An information leak was discovered on Yubico YubiKey 5 NFC devices 5.0.0 to 5.2.6 and 5.3.0 to 5.3.1. The OTP application allows a user to set optional access codes on OTP slots. This access code is intended to prevent unauthorized changes to OTP configurations. The access code is not checked when updating NFC specific components of the OTP configurations. This may allow an attacker to access configured OTPs and passwords stored in slots that were not configured by the user to be read over NFC, despite a user having set an access code. (Users who have not set an access code, or who have not configured the OTP slots, are not impacted by this issue.)	5.3	More Details
CVE-2020-11081	osquery before version 4.4.0 enables a privilege escalation vulnerability. If a Window system is configured with a PATH that contains a user-writable directory then a local user may write a zlib1.dll DLL, which osquery will attempt to load. Since osquery runs with elevated privileges this enables local escalation. This is fixed in version 4.4.0.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1434	An elevation of privilege vulnerability exists in the way that the Windows Sync Host Service handles objects in memory, aka 'Windows Sync Host Service Elevation of Privilege Vulnerability'.	5.3	More Details
CVE-2019-20899	The Gadget API in Atlassian Jira Server and Data Center in affected versions allows remote attackers to make Jira unresponsive via repeated requests to a certain endpoint in the Gadget API. The affected versions are before version 8.5.4, and from version 8.6.0 before 8.6.1.	5.3	More Details
CVE-2020-12405	When browsing a malicious page, a race condition in our SharedWorkerService could occur and lead to a potentially exploitable crash. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.	5.3	More Details
CVE-2020-6286	The insufficient input path validation of certain parameter in the web service of SAP NetWeaver AS JAVA (LM Configuration Wizard), versions - 7.30, 7.31, 7.40, 7.50, allows an unauthenticated attacker to exploit a method to download zip files to a specific directory, leading to Path Traversal.	5.3	More Details
CVE-2020-7588	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions < V3.3), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions < V2.6), SIMATIC IT Production Suite (All versions < V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions < V3.0 SP1), SIMATIC STEP 7 (TIA Portal) V15 (All versions < V15.1 Update 5), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES V15.1 (All versions < V15.1 Update 4), SIMOCODE ES V16 (All versions < V16 Update 1), Soft Starter ES V15.1 (All versions < V15.1 Update 3), Soft Starter ES V16 (All versions < V16 Update 1). Sending a specially crafted packet to the affected service could cause a partial remote denial-of-service, that would cause the service to restart itself.	5.3	More Details
CVE-2020-1267	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2031	An integer underflow vulnerability in the dnsproxyd component of the PAN-OS management interface allows authenticated administrators to issue a command from the command line interface that causes the component to stop responding. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode. This issue impacts: PAN-OS 9.1 versions earlier than PAN-OS 9.1.3. This issue does not impact PAN-OS 8.1, PAN-OS 9.0, or Prisma Access services.	4.9	More Details
CVE-2019-20900	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the Add Field module. The affected versions are before version 8.7.0.	4.8	More Details
CVE-2020-1982	Certain communication between PAN-OS and cloud-delivered services inadvertently use TLS 1.0, which is known to be a cryptographically weak protocol. These cloud services include Cortex Data Lake, the Customer Support Portal, and the Prisma Access infrastructure. Conditions required for exploitation of known TLS 1.0 weaknesses do not exist for the communication between PAN-OS and cloud-delivered services. We do not believe that any communication is impacted as a result of known attacks against TLS 1.0. This issue impacts: All versions of PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.14; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 9.1 versions earlier than PAN-OS 9.1.3. PAN-OS 7.1 is not impacted by this issue.	4.8	More Details
CVE-2020-13132	An issue was discovered in Yubico libykpiv before 2.1.0. An attacker can trigger an incorrect free() in the ykpiv_util_generate_key() function in lib/util.c through incorrect error handling code. This could be used to cause a denial of service attack.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15104	In Envoy before versions 1.12.6, 1.13.4, 1.14.4, and 1.15.0 when validating TLS certificates, Envoy would incorrectly allow a wildcard DNS Subject Alternative Name apply to multiple subdomains. For example, with a SAN of *.example.com, Envoy would incorrectly allow nested.subdomain.example.com, when it should only allow subdomain.example.com. This defect applies to both validating a client TLS certificate in mTLS, and validating a server TLS certificate for upstream connections. This vulnerability is only applicable to situations where an untrusted entity can obtain a signed wildcard TLS certificate for a domain of which you only intend to trust a subdomain of. For example, if you intend to trust api.mysubdomain.example.com, and an untrusted actor can obtain a signed TLS certificate for *.example.com or *.com. Configurations are vulnerable if they use verify_subject_alt_name in any Envoy version, or if they use match_subject_alt_names in version 1.14 or later. This issue has been fixed in Envoy versions 1.12.6, 1.13.4, 1.14.4, 1.15.0.	4.6	More Details
CVE-2020-12399	NSS has shown timing differences when performing DSA signatures, which was exploitable and could eventually leak private keys. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.	4.4	More Details
CVE-2020-12402	During RSA key generation, bignum implementations used a variation of the Binary Extended Euclidean Algorithm which entailed significantly input-dependent flow. This allowed an attacker able to perform electromagnetic-based side channel attacks to record traces leading to the recovery of the secret primes. *Note:* An unmodified Firefox browser does not generate RSA keys in normal operation and is not affected, but products built on top of it might. This vulnerability affects Firefox < 78.	4.4	More Details
CVE-2020-4173	IBM Guardium Activity Insights 10.6 and 11.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 174682.	4.3	More Details
CVE-2020-14170	Webhooks in Atlassian Bitbucket Server from version 5.4.0 before version 7.3.1 allow remote attackers to access the content of internal network resources via a Server-Side Request Forgery (SSRF) vulnerability.	4.3	More Details
CVE-2020-12412	By navigating a tab using the history API, an attacker could cause the address bar to display the incorrect domain (with the https:// scheme, a blocked port number such as '1', and without a lock icon) while controlling the page contents. This vulnerability affects Firefox < 70.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1462	An information disclosure vulnerability exists when Skype for Business is accessed via Microsoft Edge (EdgeHTML-based), aka 'Skype for Business via Microsoft Edge (EdgeHTML-based) Information Disclosure Vulnerability'.	4.3	More Details
CVE-2020-14174	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to view titles of a private project via an Insecure Direct Object References (IDOR) vulnerability in the Administration Permission Helper. The affected versions are before version 7.13.6, from version 8.0.0 before 8.5.7, from version 8.6.0 before 8.9.2, and from version 8.10.0 before 8.10.1.	4.3	More Details
CVE-2020-13131	An issue was discovered in Yubico libykpiv before 2.1.0. lib/util.c in this library (which is included in yubico-piv-tool) does not properly check embedded length fields during device communication. A malicious PIV token can misreport the returned length fields during RSA key generation. This will cause stack memory to be copied into heap allocated memory that gets returned to the caller. The leaked memory could include PINs, passwords, key material, and other sensitive information depending on the integration. During further processing by the caller, this information could leak across trust boundaries. Note that RSA key generation is triggered by the host and cannot directly be triggered by the token.	4.3	More Details
CVE-2020-1432	An information disclosure vulnerability exists when Skype for Business is accessed via Internet Explorer, aka 'Skype for Business via Internet Explorer Information Disclosure Vulnerability'.	4.3	More Details
CVE-2020-8181	A missing file type check in Nextcloud Contacts 3.2.0 allowed a malicious user to upload any file as avatars.	4.3	More Details
CVE-2020-8196	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users.	4.3	More Details
CVE-2020-1444	A remote code execution vulnerability exists in the way Microsoft SharePoint software parses specially crafted email messages, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'.	4.3	More Details
CVE-2020-12404	For native-to-JS bridging the app requires a unique token to be passed that ensures non-app code can't call the bridging functions. That token could leak when used for downloading files. This vulnerability affects Firefox for iOS < 26.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15719	libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the third-party package is asserting RFC6125 support. It considers CN even when there is a non-matching subjectAltName (SAN). This is fixed in, for example, openldap-2.4.46-10.el8 in Red Hat Enterprise Linux.	4.2	More Details
CVE-2020-11083	In October from version 1.0.319 and before version 1.0.466, a user with access to a markdown FormWidget that stores data persistently could create a stored XSS attack against themselves and any other users with access to the generated HTML from the field. This has been fixed in 1.0.466. For users of the RainLab.Blog plugin, this has also been fixed in 1.4.1.	3.5	More Details
CVE-2020-12025	Rockwell Automation Logix Designer Studio 5000 Versions 32.00, 32.01, and 32.02 vulnerable to an xml external entity (XXE) vulnerability, which may allow an attacker to view hostnames or other resources from the program.	3.3	More Details
CVE-2020-15100	In freewvs before 0.1.1, a user could create a large file that freewvs will try to read, which will terminate a scan process. This has been patched in 0.1.1.	2.8	More Details
CVE-2020-15101	In freewvs before 0.1.1, a directory structure of more than 1000 nested directories can interrupt a freewvs scan due to Python's recursion limit and os.walk(). This can be problematic in a case where an administrator scans the dirs of potentially untrusted users. This has been patched in 0.1.1.	2.8	More Details
CVE-2020-6280	SAP NetWeaver (ABAP Server) and ABAP Platform, versions 731, 740, 750, allows an attacker with admin privileges to access certain files which should otherwise be restricted, leading to Information Disclosure.	2.7	More Details
CVE-2020-14476	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-2019-15882	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 2019. Notes: none	N/A	More Details
CVE-2012-6473	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 2012. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2012-6474	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 2012. Notes: none	N/A	More Details
CVE-2019-15885	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 2019. Notes: none	N/A	More Details
CVE-2019-15886	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 2019. Notes: none	N/A	More Details
CVE-2019-15887	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 2019. Notes: none	N/A	More Details
CVE-2019-15888	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 2019. Notes: none	N/A	More Details
CVE-2019-15881	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 2019. Notes: none	N/A	More Details
CVE-2019-10096	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-11992	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2019-15884	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 2019. Notes: none	N/A	More Details
CVE-2020-13983	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-14159. Reason: This candidate is a reservation duplicate of CVE-2020-14159. Notes: All CVE users should reference CVE-2020-14159 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2013-1703	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 2013. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-0802	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 2013. Notes: none	N/A	More Details
CVE-2012-6492	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 2012. Notes: none	N/A	More Details
CVE-2012-6491	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 2012. Notes: none	N/A	More Details
CVE-2012-6490	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 2012. Notes: none	N/A	More Details
CVE-2012-6489	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 2012. Notes: none	N/A	More Details
CVE-2012-6488	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 2012. Notes: none	N/A	More Details
CVE-2012-6487	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 2012. Notes: none	N/A	More Details
CVE-2012-6486	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 2012. Notes: none	N/A	More Details
CVE-2012-6485	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 2012. Notes: none	N/A	More Details
CVE-2012-6484	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 2012. Notes: none	N/A	More Details
CVE-2012-6483	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 2012. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2012-6482	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 2012. Notes: none	N/A	More Details
CVE-2012-6481	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 2012. Notes: none	N/A	More Details
CVE-2012-6480	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 2012. Notes: none	N/A	More Details
CVE-2012-6479	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 2012. Notes: none	N/A	More Details
CVE-2012-6478	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 2012. Notes: none	N/A	More Details
CVE-2012-6477	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 2012. Notes: none	N/A	More Details
CVE-2012-6476	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 2012. Notes: none	N/A	More Details
CVE-2012-6475	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 2012. Notes: none	N/A	More Details
CVE-2019-15883	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 2019. Notes: none	N/A	More Details