SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 16 September 2020

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-25213	The File Manager (wp-file-manager) plugin before 6.9 for WordPress allows remote attackers to upload and execute arbitrary PHP code because it renames an unsafe example elFinder connector file to have the .php extension. This, for example, allows attackers to run the elFinder upload (or mkfile and put) command to write PHP code into the wp-content/plugins/wp-file-manager/lib/files/ directory. This was exploited in the wild in August and September 2020.	10.0	More Details
CVE-2020-1210	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages.	9.9	More Details
CVE-2020-16096	In Gallagher Command Centre versions 8.10 prior to 8.10.1134(MR4), 8.00 prior to 8.00.1161(MR5), 7.90 prior to 7.90.991(MR5), 7.80 prior to 7.80.960(MR2), 7.70 and earlier, any operator account has access to all data that would be replicated if the system were to be (or is) attached to a multi-server environment. This can include plain text credentials for DVR systems and card details used for physical access/alarm/perimeter components.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1595	A remote code execution vulnerability exists in Microsoft SharePoint where APIs aren't properly protected from unsafe data input. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user access a susceptible API on an affected version of SharePoint with specially-formatted input. The security update addresses the vulnerability by correcting how SharePoint handles deserialization of untrusted data.	9.9	More Details
CVE-2020-14100	In Xiaomi router R3600 ROM version<1.0.66, filters in the set_WAN6 interface can be bypassed, causing remote code execution. The router administrator can gain root access from this vulnerability.	9.8	More Details
CVE-2020-25575	An issue was discovered in the failure crate through 0.1.5 for Rust. It may introduce "compatibility hazards" in some applications, and has a type confusion flaw when downcasting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: This may overlap CVE-2019-25010	9.8	More Details
CVE-2020-25257	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. It allows XXE attacks for read/write access to arbitrary files.	9.8	More Details
CVE-2020-24074	The decode program in silk-v3-decoder Version:20160922 Build By kn007 does not strictly check data, resulting in a buffer overflow.	9.8	More Details
CVE-2020-25259	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. It uses XML deserialization libraries in an unsafe manner.	9.8	More Details
CVE-2020-25260	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. It allows remote attackers to execute arbitrary code because of unsafe JSON deserialization.	9.8	More Details
CVE-2020-14096	Memory overflow in Xiaomi AI speaker Rom version <1.59.6 can happen when the speaker verifying a malicious firmware during OTA process.	9.8	More Details
CVE-2020-25258	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. It uses ASP.NET BinaryFormatter.Deserialize in a manner that allows attackers to transmit and execute bytecode in SOAP messages.	9.8	More Details
CVE-2020-25253	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. It allows SQL injection, as demonstrated by the TableName, ColumnName, Name, UserId, or Password parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25278	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The Quram image codec library allows attackers to overwrite memory and execute arbitrary code via crafted JPEG data that is mishandled during decoding. The Samsung IDs are SVE-2020-18088, SVE-2020-18225, SVE-2020-18301 (September 2020).	9.8	More Details
CVE-2020-25279	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos chipsets) software. The baseband component has a buffer overflow via an abnormal SETUP message, leading to execution of arbitrary code. The Samsung ID is SVE-2020-18098 (September 2020).	9.8	More Details
CVE-2020-25282	An issue was discovered on LG mobile devices with Android OS 10 software. The lguicc software (for the LG Universal Integrated Circuit Card) allows attackers to bypass intended access restrictions on property values. The LG ID is LVE-SMP-200020 (September 2020).	9.8	More Details
CVE-2020-25283	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10 software. BT manager allows attackers to bypass intended access restrictions on a certain mode. The LG ID is LVE-SMP-200021 (September 2020).	9.8	More Details
CVE-2020-24660	An issue was discovered in LemonLDAP::NG through 2.0.8, when NGINX is used. An attacker may bypass URL-based access control to protected Virtual Hosts by submitting a non-normalized URI. This also affects versions before 0.5.2 of the "Lemonldap::NG handler for Node.js" package.	9.8	More Details
CVE-2018-20432	D-Link COVR-2600R and COVR-3902 Kit before 1.01b05Beta01 use hardcoded credentials for telnet connection, which allows unauthenticated attackers to gain privileged access to the router, and to extract sensitive data or modify the configuration.	9.8	More Details
CVE-2020-25254	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. It allows SQL injection, as demonstrated by TestConnection_LocalOrLinkedServer, CreateFilterFriendlyView, or AddWorkViewLinkedServer.	9.8	More Details
CVE-2020-11998	A regression has been introduced in the commit preventing JMX re-bind. By passing an empty environment map to RMIConnectorServer, instead of the map that contains the authentication credentials, it leaves ActiveMQ open to the following attack: https://docs.oracle.com/javase/8/docs/technotes/guides/management/agent.html "A remote client could create a javax.management.loading.MLet MBean and use it to create new MBeans from arbitrary URLs, at least if there is no security manager. In other words, a rogue remote client could make your Java application execute arbitrary code." Mitigation: Upgrade to Apache ActiveMQ 5.15.13	9.8	More Details
CVE-2020-25576	An issue was discovered in the rand_core crate before 0.4.2 for Rust. Casting of byte slices to integer slices mishandles alignment constraints.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-0230	Apache Struts 2.0.0 to 2.5.20 forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution.	9.8	More Details
CVE-2020-24197	A SQL injection vulnerability in the login component in Stock Management System v1.0 allows remote attacker to execute arbitrary SQL commands via the username parameter.	9.8	More Details
CVE-2020-23833	Projectworlds House Rental v1.0 suffers from an unauthenticated SQL Injection vulnerability, allowing remote attackers to execute arbitrary code on the hosting webserver via a malicious index.php POST request.	9.8	More Details
CVE-2020-24199	Arbitrary File Upload in the Vehicle Image Upload component in Project Worlds Car Rental Management System v1.0 allows attackers to conduct remote code execution.	9.8	More Details
CVE-2020-11986	To be able to analyze gradle projects, the build scripts need to be executed. Apache NetBeans follows this pattern. This causes the code of the build script to be invoked at load time of the project. Apache NetBeans up to and including 12.0 did not request consent from the user for the analysis of the project at load time. This in turn will run potentially malicious code, from an external source, without the consent of the user.	9.8	More Details
CVE-2020-2040	A buffer overflow vulnerability in PAN-OS allows an unauthenticated attacker to disrupt system processes and potentially execute arbitrary code with root privileges by sending a malicious request to the Captive Portal or Multi-Factor Authentication interface. This issue impacts: All versions of PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 9.1 versions earlier than PAN-OS 9.1.3.	9.8	More Details
CVE-2020-15786	A vulnerability has been identified in SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions < V16), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions <= V16), SIMATIC HMI Mobile Panels (All versions <= V16), SIMATIC HMI Unified Comfort Panels (All versions <= V16). Affected devices insufficiently block excessive authentication attempts. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack.	9.8	More Details
CVE-2020-15787	A vulnerability has been identified in SIMATIC HMI Unified Comfort Panels (All versions <= V16). Affected devices insufficiently validate authentication attempts as the information given can be truncated to match only a set number of characters versus the whole provided string. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack.	9.8	More Details
CVE-2020-24379	WebDAV implementation in Yaws web server versions 1.81 to 2.0.7 is vulnerable to XXE injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24916	CGI implementation in Yaws web server versions 1.81 to 2.0.7 is vulnerable to OS command injection.	9.8	More Details
CVE-2020-15903	An issue was found in Nagios XI before 5.7.3. There is a privilege escalation vulnerability in backend scripts that ran as root where some included files were editable by nagios user. This issue was fixed in version 5.7.3.	9.8	More Details
CVE-2020-8758	Improper buffer restrictions in network subsystem in provisioned Intel(R) AMT and Intel(R) ISM versions before 11.8.79, 11.12.79, 11.22.79, 12.0.68 and 14.0.39 may allow an unauthenticated user to potentially enable escalation of privilege via network access. On un-provisioned systems, an authenticated user may potentially enable escalation of privilege via local access.	9.8	More Details
CVE-2020-23828	A File Upload vulnerability in SourceCodester Online Course Registration v1.0 allows remote attackers to achieve Remote Code Execution (RCE) on the hosting webserver by uploading a crafted PHP web-shell that bypasses the image upload filters. An attack uses /Online%20Course%20Registration/my-profile.php with the POST parameter photo.	9.8	More Details
CVE-2020-23512	VR CAM P1 Model P1 v1 has an incorrect access control vulnerability where an attacker can obtain complete access of the device from web (remote) without authentication.	9.8	More Details
CVE-2020-16098	It is possible to enumerate access card credentials via an unauthenticated network connection to the server in versions of Command Centre v8.20 prior to v8.20.1166(MR3), versions of 8.10 prior to v8.10.1211(MR5), versions of 8.00 prior to v8.00.1228(MR6), all versions of 7.90 and earlier. These credentials can then be used to encode low security cards to be used by the system where insecure card technologies are supported.	9.8	More Details
CVE-2020-25573	An issue was discovered in the linked-hash-map crate before 0.5.3 for Rust. It creates an uninitialized NonNull pointer, which violates a non-null constraint.	9.8	More Details
CVE-2020-24561	A command injection vulnerability in Trend Micro ServerProtect for Linux 3.0 could allow an attacker to execute arbitrary code on an affected system. An attacker must first obtain admin/root privileges on the SPLX console to exploit this vulnerability.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3634	u'Multiple Read overflows issue due to improper length check while decoding Generic NAS transport/EMM info' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details
CVE-2020-11684	AT91bootstrap before 3.9.2 does not properly wipe encryption and authentication keys from memory before passing control to a less privileged software component. This can be exploited to disclose these keys and subsequently encrypt and sign the next boot stage (such as the bootloader).	9.1	More Details
CVE-2020-25256	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. PKI certificates have a private key that is the same across different customers' installations.	9.1	More Details
CVE-2020-25251	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. Client-side authentication is used for critical functions such as adding users or retrieving sensitive information.	9.1	More Details
CVE-2020-24195	An Arbitrary File Upload in the Upload Image component in Sourcecodester Online Bike Rental v1.0 allows authenticated administrator to conduct remote code execution.	9.1	More Details
CVE-2020-9742	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below) and 6.3.3.8 (and below) are affected by a stored XSS vulnerability that allows users with 'Author' privileges to store malicious scripts in fields associated with the Inbox calendar feature. These scripts may be executed in a victim’s browser when they open the page containing the vulnerable field.	9.0	More Details
CVE-2020-9741	The AEM forms add-on for versions 6.5.5.0 (and below) and 6.4.8.2 (and below) is affected by a stored XSS vulnerability that allows users with 'Author' privileges to store malicious scripts in fields associated with the Forms component. These scripts may be executed in a victim’s browser when they open the page containing the vulnerable field.	9.0	More Details
CVE-2020-9740	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by a stored XSS vulnerability that allows users with 'Author' privileges to store malicious scripts in fields associated with the Design Importer. These scripts may be executed in a victim’s browser when they open the page containing the vulnerable field.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9734	The AEM Forms add-on for versions 6.5.5.0 (and below) and 6.4.8.1 (and below) is affected by a stored XSS vulnerability that allows users with 'Author' privileges to store malicious scripts in fields associated with the Forms component. These scripts may be executed in a victim’s browser when they open the page containing the vulnerable field.	9.0	More Details
CVE-2020-9732	The AEM Forms add-on for versions 6.5.5.0 (and below) and 6.4.8.2 (and below) are affected by a stored XSS vulnerability that allows users with 'Author' privileges to store malicious scripts in fields associated with the Sites component. These scripts may be executed in a victim’s browser when they open the page containing the vulnerable field.	9.0	More Details
CVE-2020-7293	Privilege Escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows authenticated user interface user with low permissions to change the system's root password via improper access controls in the user interface.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-15148	Yii 2 (yiisoft/yii2) before version 2.0.38 is vulnerable to remote code execution if the application calls `unserialize()` on arbitrary user input. This is fixed in version 2.0.38. A possible workaround without upgrading is available in the linked advisory.	8.9	More Details
CVE-2020-1523	A tampering vulnerability exists when Microsoft SharePoint Server fails to properly handle profile data. An attacker who successfully exploited this vulnerability could modify a targeted user's profile data. To exploit the vulnerability, an attacker would need to be authenticated on an affected SharePoint Server. The attacker would then need to send a specially modified request to the server, targeting a specific user. The security update addresses the vulnerability by modifying how Microsoft SharePoint Server handles profile data.	8.9	More Details
CVE-2020-0922	A remote code execution vulnerability exists in the way that Microsoft COM for Windows handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code on a target system. To exploit the vulnerability, a user would have to open a specially crafted file or lure the target to a website hosting malicious JavaScript. The security update addresses the vulnerability by correcting how Microsoft COM for Windows handles objects in memory.	8.8	More Details
CVE-2020-16222	In Patient Information Center iX (PICiX) Version B.02, C.02, C.03, and PerformanceBridge Focal Point Version A.01, when an actor claims to have a given identity, the software does not prove or insufficiently proves the claim is correct.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1129	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Exploitation of the vulnerability requires that a program process a specially crafted image file. The update addresses the vulnerability by correcting how Microsoft Windows Codecs Library handles objects in memory.	8.8	More Details
CVE-2020-25252	An issue was discovered in Hyland OnBase through 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. CSRF can be used to log in a user, and then perform actions, because there are default credentials (the wstinol password for the manager or hsi account).	8.8	More Details
CVE-2020-13127	A SQL injection vulnerability at a tpf URI in Loway QueueMetrics before 19.04.1 allows remote authenticated attackers to execute arbitrary SQL commands via the TASKS_LIST__pt.querystring parameter.	8.8	More Details
CVE-2020-4521	IBM Maximo Asset Management 7.6.0 and 7.6.1 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unsafe deserialization in Java. By sending specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 182396.	8.8	More Details
CVE-2020-23451	Spiceworks Version <= 7.5.00107 is affected by CSRF which can lead to privilege escalation via "/settings/v1/users" function.	8.8	More Details
CVE-2020-2036	A reflected cross-site scripting (XSS) vulnerability exists in the PAN-OS management web interface. A remote attacker able to convince an administrator with an active authenticated session on the firewall management interface to click on a crafted link to that management web interface could potentially execute arbitrary JavaScript code in the administrator's browser and perform administrative actions. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9.	8.8	More Details
CVE-2020-23824	ArGo Soft Mail Server 1.8.8.9 is affected by Cross Site Request Forgery (CSRF) for perform remote arbitrary code execution. The component is the Administration dashboard. When using admin/user credentials, if the admin/user admin opens a website with the malicious page that will run the CSRF.	8.8	More Details
CVE-2020-10229	A CSRF issue in vtecrm vtenext 19 CE allows attackers to carry out unwanted actions on an administrator's behalf, such as uploading files, adding users, and deleting accounts.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0761	A remote code execution vulnerability exists when Active Directory integrated DNS (ADIDNS) mishandles objects in memory. An authenticated attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account To exploit the vulnerability, an authenticated attacker could send malicious requests to an Active Directory integrated DNS (ADIDNS) server. The update addresses the vulnerability by correcting how Active Directory integrated DNS (ADIDNS) handles objects in memory.	8.8	More Details
CVE-2020-7319	Improper Access Control vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local users to access files which the user otherwise would not have access to via manipulating symbolic links to redirect McAfee file operations to an unintended file.	8.8	More Details
CVE-2020-0718	A remote code execution vulnerability exists when Active Directory integrated DNS (ADIDNS) mishandles objects in memory. An authenticated attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account To exploit the vulnerability, an authenticated attacker could send malicious requests to an Active Directory integrated DNS (ADIDNS) server. The update addresses the vulnerability by correcting how Active Directory integrated DNS (ADIDNS) handles objects in memory.	8.8	More Details
CVE-2020-10228	A file upload vulnerability in vtecrm vtenext 19 CE allows authenticated users to upload files with a .pht extension, resulting in remote code execution.	8.8	More Details
CVE-2020-25453	An issue was discovered in BlackCat CMS before 1.4. There is a CSRF vulnerability (bypass csrf_token) that allows remote arbitrary code execution.	8.8	More Details
CVE-2020-25379	Wordpress Plugin Store / Mike Rooijackers Recall Products V0.8 fails to sanitize input from the 'Manufacturer[]' parameter which allows an authenticated attacker to inject a malicious SQL query.	8.8	More Details
CVE-2020-1012	An elevation of privilege vulnerability exists in the way that the Wininit.dll handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. There are multiple ways an attacker could exploit the vulnerability: - In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. - In a file sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit this vulnerability, and then convince a user to open the document file. The security update addresses the vulnerability by ensuring the Wininit.dll properly handles objects in memory.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15172	The Act module for Red Discord Bot before commit 6b9f3b86 is vulnerable to Remote Code Execution. With this exploit, Discord users can use specially crafted messages to perform destructive actions and/or access sensitive information. Unloading the Act module with `unload act` can render this exploit inaccessible.	8.7	More Details
CVE-2020-15163	Python TUF (The Update Framework) reference implementation before version 0.12 it will incorrectly trust a previously downloaded root metadata file which failed verification at download time. This allows an attacker who is able to serve multiple new versions of root metadata (i.e. by a person-in-the-middle attack) culminating in a version which has not been correctly signed to control the trust chain for future updates. This is fixed in version 0.12 and newer.	8.7	More Details
CVE-2020-1200	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages.	8.6	More Details
CVE-2020-1452	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages.	8.6	More Details
CVE-2020-1453	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages.	8.6	More Details
CVE-2020-1460	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls. An authenticated attacker who successfully exploited the vulnerability could use a specially crafted page to perform actions in the security context of the SharePoint application pool process. To exploit the vulnerability, an authenticated user must create and invoke a specially crafted page on an affected version of Microsoft SharePoint Server. The security update addresses the vulnerability by correcting how Microsoft SharePoint Server handles processing of created content.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1576	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages.	8.5	More Details
CVE-2020-1285	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. There are multiple ways an attacker could exploit the vulnerability: - In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to open an email attachment or click a link in an email or instant message. - In a file-sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit the vulnerability, and then convince users to open the document file. The security update addresses the vulnerability by correcting the way that the Windows GDI handles objects in the memory.	8.4	More Details
CVE-2020-16875	A remote code execution vulnerability exists in Microsoft Exchange server due to improper validation of cmdlet arguments. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the System user. Exploitation of the vulnerability requires an authenticated user in a certain Exchange role to be compromised. The security update addresses the vulnerability by correcting how Microsoft Exchange handles cmdlet arguments.	8.4	More Details
CVE-2020-9416	The Spotfire client component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Desktop, and TIBCO Spotfire Server contains a vulnerability that theoretically allows a legitimate user to inject scripts. If executed by a victim authenticated to the affected system these scripts will be executed at the privileges of the victim. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 10.7.0, 10.8.0, 10.9.0, and 10.10.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 10.7.0, 10.8.0, 10.8.1, 10.9.0, 10.10.0, and 10.10.1, TIBCO Spotfire Desktop: versions 10.7.0, 10.8.0, 10.9.0, and 10.10.0, and TIBCO Spotfire Server: versions 10.7.0, 10.8.0, 10.8.1, 10.9.0, 10.10.0, and 10.10.1.	8.2	More Details
CVE-2020-7314	Privilege Escalation Vulnerability in the installer in McAfee Data Exchange Layer (DXL) Client for Mac shipped with McAfee Agent (MA) for Mac prior to MA 5.6.6 allows local users to run commands as root via incorrectly applied permissions on temporary files.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15173	In ACCEL-PPP (an implementation of PPTP/PPPoE/L2TP/SSTP), there is a buffer overflow when receiving an l2tp control packet ith an AVP which type is a string and no hidden flags, length set to less than 6. If your application is used in open networks or there are untrusted nodes in the network it is highly recommended to apply the patch. The problem was patched with commit 2324bcd5ba12cf28f47357a8f03cd41b7c04c52b As a workaround changes of commit 2324bcd5ba12cf28f47357a8f03cd41b7c04c52b can be applied to older versions.	8.2	More Details
CVE-2020-15789	A vulnerability has been identified in Polarion Subversion Webclient (All versions). The web interface could allow a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link. Successful exploitation requires user interaction by a legitimate user, who must be authenticated to the web interface. A successful attack could allow an attacker to trigger actions via the web interface that the legitimate user is allowed to perform. This could allow the attacker to read or modify contents of the web application.	8.1	More Details
CVE-2020-8817	Dataiku DSS before 6.0.5 allows attackers write access to the project to modify the "Created by" metadata.	8.1	More Details
CVE-2020-6320	SAP Marketing (Servlet), version-130,140,150, allows an authenticated attacker to invoke certain functions that are restricted. Limited knowledge of payload is required for an attacker to exploit the vulnerability and perform tasks related to contact and interaction data which impacts Confidentiality and Integrity of data in the application.	8.1	More Details
CVE-2020-6302	SAP Commerce versions 6.7, 1808, 1811, 1905, 2005 contains the jSession ID in the backoffice URL when the application is loaded initially. An attacker can get this session ID via shoulder surfing or man in the middle attack and subsequently get access to admin user accounts, leading to Session Fixation and complete compromise of the confidentiality, integrity and availability of the application.	8.1	More Details
CVE-2020-1912	An out-of-bounds read/write vulnerability when executing lazily compiled inner generator functions in Facebook Hermes prior to commit 091835377369c8fd5917d9b87acffa721ad2a168 allows attackers to potentially execute arbitrary code via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected.	8.1	More Details
CVE-2020-1913	An Integer signedness error in the JavaScript Interpreter in Facebook Hermes prior to commit 2c7af7ec481ceffd0d14ce2d7c045e475fd71dc6 allows attackers to cause a denial of service attack or a potential RCE via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected.	8.1	More Details
CVE-2020-13299	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. The revocation feature was not revoking all session tokens and one could re-use it to obtain a valid session.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13300	GitLab CE/EE version 13.3 prior to 13.3.4 was vulnerable to an OAuth authorization scope change without user consent in the middle of the authorization flow.	8.0	More Details
CVE-2020-15179	The ScratchSig extension for MediaWiki before version 1.0.1 allows stored Cross-Site Scripting. Using <script> tag inside <scratchsig> tag, attackers with edit permission can execute scripts on visitors' browser. With MediaWiki JavaScript API, this can potentially lead to privilege escalation and/or account takeover. This has been patched in release 1.0.1. This has already been deployed to all Scratch Wikis. No workarounds exist other than disabling the extension completely.	8.0	More Details
CVE-2020-4703	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 Administrative Console could allow an authenticated attacker to upload arbitrary files which could be execute arbitrary code on the vulnerable server. This vulnerability is due to an incomplete fix for CVE-2020-4470. IBM X-Force ID: 187188.	8.0	More Details
CVE-2020-15178	In PrestaShop contactform module (prestashop/contactform) before version 4.3.0, an attacker is able to inject JavaScript while using the contact form. The `message` field was incorrectly unescaped, possibly allowing attackers to execute arbitrary JavaScript in a victim's browser.	8.0	More Details
CVE-2020-1507	An elevation of privilege vulnerability exists in the way that Microsoft COM for Windows handles objects in memory. An attacker who successfully exploited the vulnerability could gain elevated privileges on a targeted system. To exploit the vulnerability, a user would have to open a specially crafted file. The security update addresses the vulnerability by correcting how Microsoft COM for Windows handles objects in memory.	7.9	More Details
CVE-2020-1338	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. To exploit the vulnerability, a user must open a specially crafted file with an affected version of Microsoft Word software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Word handles files in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9725	Adobe FrameMaker version 2019.0.6 (and earlier versions) lacks proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. This could be exploited to execute arbitrary code with the privileges of the current user. User interaction is required to exploit this vulnerability in that the target must open a malicious FrameMaker file.	7.8	More Details
CVE-2020-1376	An elevation of privilege vulnerability exists in the way that fdSSDP.dll 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 ssdpsrv.dll properly handles objects in memory.	7.8	More Details
CVE-2020-14363	An integer overflow vulnerability leading to a double-free was found in libX11. This flaw allows a local privileged attacker to cause an application compiled with libX11 to crash, or in some cases, result in arbitrary code execution. The highest threat from this flaw is to confidentiality, integrity as well as system availability.	7.8	More Details
CVE-2020-25221	get_gate_page in mm/gup.c in the Linux kernel 5.7.x and 5.8.x before 5.8.7 allows privilege escalation because of incorrect reference counting (caused by gate page mishandling) of the struct page that backs the vsyscall page. The result is a refcount underflow. This can be triggered by any 64-bit process that can use ptrace() or process_vm_readv(), aka CID-9fa2dd946743.	7.8	More Details
CVE-2020-1491	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service 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 Function Discovery Service properly handles objects in memory.	7.8	More Details
CVE-2020-1532	An elevation of privilege vulnerability exists when the Windows InstallService improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows InstallService handles memory.	7.8	More Details
CVE-2020-1559	An elevation of privilege vulnerability exists when the Windows Storage Services improperly handle file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges. To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Storage Services properly handle file operations.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1030	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application. The update addresses the vulnerability by correcting how the Windows Print Spooler Component writes to the file system.	7.8	More Details
CVE-2020-9728	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user.	7.8	More Details
CVE-2020-25291	GdiDrawHoriLineIAlt in Kingsoft WPS Office before 11.2.0.9403 allows remote heap corruption via a crafted PLTE chunk in PNG data within a Word document. This is related to QBrush::setMatrix in gui/painting/qbrush.cpp in Qt 4.x.	7.8	More Details
CVE-2020-7312	DLL Search Order Hijacking Vulnerability in the installer in McAfee Agent (MA) for Windows prior to 5.6.6 allows local users to execute arbitrary code and escalate privileges via execution from a compromised folder.	7.8	More Details
CVE-2020-7311	Privilege Escalation vulnerability in the installer in McAfee Agent (MA) for Windows prior to 5.6.6 allows local users to assume SYSTEM rights during the installation of MA via manipulation of log files.	7.8	More Details
CVE-2020-25220	The Linux kernel 4.9.x before 4.9.233, 4.14.x before 4.14.194, and 4.19.x before 4.19.140 has a use-after-free because skcd->no_refcnt was not considered during a backport of a CVE-2020-14356 patch. This is related to the cgroups feature.	7.8	More Details
CVE-2020-10056	A vulnerability has been identified in License Management Utility (LMU) (All versions < V2.4). The lmgrd service of the affected application is executed with local SYSTEM privileges on the server while its configuration can be modified by local users. The vulnerability could allow a local authenticated attacker to execute arbitrary commands on the server with local SYSTEM privileges.	7.8	More Details
CVE-2020-9727	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user.	7.8	More Details
CVE-2020-11124	u'Possible use-after-free while accessing diag client map table since list can be reallocated due to exceeding max client limit.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCS404, QCS405, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9729	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user.	7.8	More Details
CVE-2020-1169	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory.	7.8	More Details
CVE-2020-16881	A remote code execution vulnerability exists in Visual Studio Code when a user is tricked into opening a malicious 'package.json' file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to convince a target to clone a repository and open it in Visual Studio Code. Attacker-specified code would execute when the target opens the malicious 'package.json' file. The update address the vulnerability by modifying the way Visual Studio Code handles JSON files.	7.8	More Details
CVE-2020-1039	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.	7.8	More Details
CVE-2020-16874	A remote code execution vulnerability exists in Visual Studio when it improperly handles objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted file with an affected version of Visual Studio. The update addresses the vulnerability by correcting how Visual Studio handles objects in memory.	7.8	More Details
CVE-2020-1052	An elevation of privilege vulnerability exists in the way that the ssdpsrv.dll 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 ssdpsrv.dll properly handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1053	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how DirectX handles objects in memory.	7.8	More Details
CVE-2020-1074	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.	7.8	More Details
CVE-2020-16856	A remote code execution vulnerability exists in Visual Studio when it improperly handles objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted file with an affected version of Visual Studio. The update addresses the vulnerability by correcting how Visual Studio handles objects in memory.	7.8	More Details
CVE-2020-1098	An elevation of privilege vulnerability exists when the Shell infrastructure component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting the way in which the Shell infrastructure component handles objects in memory and preventing unintended elevation from lower integrity application.	7.8	More Details
CVE-2020-1115	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system. The security update addresses the vulnerability by correcting how CLFS handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0998	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take control over the affected system. The update addresses the vulnerability by correcting the way in which the Microsoft Graphics Component handles objects in memory and preventing unintended elevation from user mode.	7.8	More Details
CVE-2020-0997	A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of the Windows Camera Codec Pack. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how the Windows Camera Codec Pack handles objects in memory.	7.8	More Details
CVE-2020-11129	u'During the error occurrence in capture request, the buffer is freed and later accessed causing the camera APP to fail due to memory use-after-free' in Snapdragon Consumer IOT, Snapdragon Mobile in Bitra, Kamorta, QCS605, Saipan, SDM710, SM8250, SXR2130	7.8	More Details
CVE-2020-0911	An elevation of privilege vulnerability exists when Windows Modules Installer improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Modules Installer handles objects in memory.	7.8	More Details
CVE-2020-0886	An elevation of privilege vulnerability exists when the Windows Storage Services improperly handle file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges. To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Storage Services properly handle file operations.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0870	An elevation of privilege vulnerability exists when the Shell infrastructure component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting the way in which the Shell infrastructure component handles objects in memory and preventing unintended elevation from lower integrity application.	7.8	More Details
CVE-2020-9730	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user.	7.8	More Details
CVE-2020-0839	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll 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 dnsrslvr.dll properly handles objects in memory.	7.8	More Details
CVE-2020-0838	An elevation of privilege vulnerability exists when NTFS improperly checks access. An attacker who successfully exploited this vulnerability could run processes in an elevated context. To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system. The security update addresses the vulnerability by correcting how NTFS checks access.	7.8	More Details
CVE-2020-1193	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0790	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls. An attacker who successfully exploited the vulnerability could elevate privileges on an affected system from low-integrity to medium-integrity. This vulnerability by itself does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability (such as a remote code execution vulnerability or another elevation of privilege vulnerability) that is capable of leveraging the elevated privileges when code execution is attempted. The security update addresses the vulnerability by ensuring splwow64.exe properly handles these calls..	7.8	More Details
CVE-2020-0782	An elevation of privilege vulnerability exists when the Windows Cryptographic Catalog Services improperly handle objects in memory. An attacker who successfully exploited this vulnerability could modify the cryptographic catalog. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by addressing how the Windows Cryptographic Catalog Services handle objects in memory.	7.8	More Details
CVE-2020-0766	An elevation of privilege vulnerability exists when the Microsoft Store Runtime improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Microsoft Store Runtime handles memory.	7.8	More Details
CVE-2020-0648	An elevation of privilege vulnerability exists when the Windows RSoP Service Application improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows RSoP Service Application handles memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1218	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. To exploit the vulnerability, a user must open a specially crafted file with an affected version of Microsoft Word software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Word handles files in memory.	7.8	More Details
CVE-2020-1252	A remote code execution vulnerability exists when Windows improperly handles objects in memory. To exploit the vulnerability an attacker would have to convince a user to run a specially crafted application. An attacker who successfully exploited this vulnerability could execute arbitrary code and take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The updates address the vulnerability by correcting how Windows handles objects in memory.	7.8	More Details
CVE-2020-10050	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.10.2). The directory of service executables of the affected application could allow a local attacker to include arbitrary commands that are executed with SYSTEM privileges when the system restarts.	7.8	More Details
CVE-2020-24164	A deserialization flaw is present in Taoensso Nippy before 2.14.2. In some circumstances, it is possible for an attacker to create a malicious payload that, when deserialized, will allow arbitrary code to be executed. This occurs because there is automatic use of the Java Serializable interface.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1332	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	7.8	More Details
CVE-2020-1335	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	7.8	More Details
CVE-2020-9731	A memory corruption vulnerability exists in InDesign 15.1.1 (and earlier versions). Insecure handling of a malicious indd file could be abused to cause an out-of-bounds memory access, potentially resulting in code execution in the context of the current user.	7.8	More Details
CVE-2020-10051	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.10.2). Multiple services of the affected application are executed with SYSTEM privileges while the call path is not quoted. This could allow a local attacker to inject arbitrary commands that are exeeceuted instead of the legitimate service.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1594	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.	7.8	More Details
CVE-2020-14361	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Integer underflow leading to heap-buffer overflow may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2020-3656	Out of bound access can happen in MHI command process due to lack of check of command channel id value received from MHI devices in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2020-14362	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Integer underflow leading to heap-buffer overflow may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2020-14345	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Out-Of-Bounds access in XkbSetNames function may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2020-14346	A flaw was found in xorg-x11-server before 1.20.9. An integer underflow in the X input extension protocol decoding in the X server may lead to arbitrary access of memory contents. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1593	A remote code execution vulnerability exists when Windows Media Audio Decoder improperly handles objects. An attacker who successfully exploited the vulnerability could take control of an affected system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Audio Decoder handles objects.	7.6	More Details
CVE-2020-16872	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	7.6	More Details
CVE-2020-1508	A remote code execution vulnerability exists when Windows Media Audio Decoder improperly handles objects. An attacker who successfully exploited the vulnerability could take control of an affected system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Audio Decoder handles objects.	7.6	More Details
CVE-2020-24457	Logic error in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processors may allow an unauthenticated user to potentially enable escalation of privilege, denial of service and/or information disclosure via physical access.	7.6	More Details
CVE-2020-16100	It is possible for an unauthenticated remote DCOM websocket connection to crash the Command Centre service's DCOM websocket thread due to improper shutdown of closed websocket connections, preventing it from accepting future DCOM websocket (Configuration Client) connections. Affected versions are v8.20 prior to v8.20.1166(MR3), v8.10 prior to v8.10.1211(MR5), v8.00 prior to v8.00.1228(MR6), all versions of 7.90 and earlier.	7.5	More Details
CVE-2020-14198	Bitcoin Core 0.20.0 allows remote denial of service.	7.5	More Details
CVE-2020-24566	In Octopus Deploy 2020.3.x before 2020.3.4 and 2020.4.x before 2020.4.1, if an authenticated user creates a deployment or runbook process using Azure steps and sets the step's execution location to run on the server/worker, then (under certain circumstances) the account password is exposed in cleartext in the verbose task logs output.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25574	An issue was discovered in the http crate before 0.1.20 for Rust. An integer overflow in HeaderMap::reserve() could result in denial of service (e.g., an infinite loop).	7.5	More Details
CVE-2020-1749	A flaw was found in the Linux kernel's implementation of some networking protocols in IPsec, such as VXLAN and GENEVE tunnels over IPv6. When an encrypted tunnel is created between two hosts, the kernel isn't correctly routing tunneled data over the encrypted link; rather sending the data unencrypted. This would allow anyone in between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.	7.5	More Details
CVE-2020-24925	A Sensitive Source Code Path Disclosure vulnerability is found in ElkarBackup v1.3.3. An attacker is able to view the path of the source code jobs/sort where entire source code path is displayed in the browser itself helping the attacker identify the code structure /app/elkarbackup/src/Binovo/ElkarBackupBundle/Controller/DefaultController.php	7.5	More Details
CVE-2020-6097	An exploitable denial of service vulnerability exists in the atftpd daemon functionality of atftp 0.7.git20120829-3.1+b1. A specially crafted sequence of RRQ-Multicast requests trigger an assert() call resulting in denial-of-service. An attacker can send a sequence of malicious packets to trigger this vulnerability.	7.5	More Details
CVE-2018-17145	Bitcoin Core 0.16.x before 0.16.2 and Bitcoin Knots 0.16.x before 0.16.2 allow remote denial of service via a flood of multiple transaction inv messages with random hashes, aka INVDoS. NOTE: this can also affect other cryptocurrencies, e.g., if they were forked from Bitcoin Core after 2017-11-15.	7.5	More Details
CVE-2020-16101	It is possible for an unauthenticated remote DCOM websocket connection to crash the Command Centre service due to an out-of-bounds buffer access. Affected versions are v8.20 prior to v8.20.1166(MR3), v8.10 prior to v8.10.1211(MR5), v8.00 prior to v8.00.1228(MR6), all versions of 7.90 and earlier.	7.5	More Details
CVE-2020-0836	A denial of service vulnerability exists in Windows DNS when it fails to properly handle queries. An attacker who successfully exploited this vulnerability could cause the DNS service to become nonresponsive. To exploit the vulnerability, an authenticated attacker could send malicious DNS queries to a target, resulting in a denial of service. The update addresses the vulnerability by correcting how Windows DNS processes queries.	7.5	More Details
CVE-2020-17408	This vulnerability allows remote attackers to disclose sensitive information on affected installations of NEC ExpressCluster 4.1. Authentication is not required to exploit this vulnerability. The specific flaw exists within the clpwebmc executable. Due to the improper restriction of XML External Entity (XXE) references, a specially-crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-10801.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15590	A vulnerability in the Private Internet Access (PIA) VPN Client for Linux 1.5 through 2.3+ allows remote attackers to bypass an intended VPN kill switch mechanism and read sensitive information via intercepting network traffic. Since 1.5, PIA has supported a “split tunnel” OpenVPN bypass option. The PIA killswitch & associated iptables firewall is designed to protect you while using the Internet. When the kill switch is configured to block all inbound and outbound network traffic, privileged applications can continue sending & receiving network traffic if net.ipv4.ip_forward has been enabled in the system kernel parameters. For example, a Docker container running on a host with the VPN turned off, and the kill switch turned on, can continue using the internet, leaking the host IP (CWE 200). In PIA 2.4.0+, policy-based routing is enabled by default and is used to direct all forwarded packets to the VPN interface automatically.	7.5	More Details
CVE-2020-9733	An AEM java servlet in AEM versions 6.5.5.0 (and below) and 6.4.8.1 (and below) executes with the permissions of a high privileged service user. If exploited, this could lead to read-only access to sensitive data in an AEM repository.	7.5	More Details
CVE-2020-15166	In ZeroMQ before version 4.3.3, there is a denial-of-service vulnerability. Users with TCP transport public endpoints, even with CURVE/ZAP enabled, are impacted. If a raw TCP socket is opened and connected to an endpoint that is fully configured with CURVE/ZAP, legitimate clients will not be able to exchange any message. Handshakes complete successfully, and messages are delivered to the library, but the server application never receives them. This is patched in version 4.3.3.	7.5	More Details
CVE-2020-11881	An array index error in MikroTik RouterOS 6.41.3 through 6.46.5, and 7.x through 7.0 Beta5, allows an unauthenticated remote attacker to crash the SMB server via modified setup-request packets, aka SUP-12964.	7.5	More Details
CVE-2020-1228	A denial of service vulnerability exists in Windows DNS when it fails to properly handle queries. An attacker who successfully exploited this vulnerability could cause the DNS service to become nonresponsive. To exploit the vulnerability, an authenticated attacker could send malicious DNS queries to a target, resulting in a denial of service. The update addresses the vulnerability by correcting how Windows DNS processes queries.	7.5	More Details
CVE-2019-0233	An access permission override in Apache Struts 2.0.0 to 2.5.20 may cause a Denial of Service when performing a file upload.	7.5	More Details
CVE-2020-14384	A flaw was found in JBossWeb in versions before 7.5.31.Final-redhat-3. The fix for CVE-2020-13935 was incomplete in JBossWeb, leaving it vulnerable to a denial of service attack when sending multiple requests with invalid payload length in a WebSocket frame. The highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2020-11991	When using the StreamGenerator, the code parse a user-provided XML. A specially crafted XML, including external system entities, could be used to access any file on the server system.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25255	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. It allows remote attackers to cause a denial of service (outage of connection-request processing) via a long user ID, which triggers an exception and a large log entry.	7.5	More Details
CVE-2020-25250	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. Client applications can write arbitrary data to the server logs.	7.5	More Details
CVE-2020-25247	An issue was discovered in Hyland OnBase through 18.0.0.32 and 19.x through 19.8.9.1000. Directory traversal exists for writing to files, as demonstrated by the FileName parameter.	7.5	More Details
CVE-2020-0908	A remote code execution vulnerability exists when the Windows Text Service Module improperly handles memory. An attacker who successfully exploited the vulnerability could gain execution on a victim system. An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (Chromium-based), and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements by adding specially crafted content that could exploit the vulnerability. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by correcting how the Windows Text Service Module handles memory.	7.5	More Details
CVE-2020-1013	An elevation of privilege vulnerability exists when Microsoft Windows processes group policy updates. An attacker who successfully exploited this vulnerability could potentially escalate permissions or perform additional privileged actions on the target machine. To exploit this vulnerability, an attacker would need to launch a man-in-the-middle (MiTM) attack against the traffic passing between a domain controller and the target machine. An attacker could then create a group policy to grant administrator rights to a standard user. The security update addresses the vulnerability by enforcing Kerberos authentication for certain calls over LDAP.	7.5	More Details
CVE-2020-25248	An issue was discovered in Hyland OnBase through 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. Directory traversal exists for reading files, as demonstrated by the FileName parameter.	7.5	More Details
CVE-2020-12789	The Secure Monitor in Microchip Atmel ATSAMA5 products use a hardcoded key to encrypt and authenticate secure applets.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11135	u'Reachable assertion when wrong data size is returned by parser for ape clips' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8098, Kamorta, MSM8917, MSM8953, Nicobar, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.5	More Details
CVE-2020-1031	An information disclosure vulnerability exists in the way that the Windows Server DHCP service improperly discloses the contents of its memory. To exploit the vulnerability, an unauthenticated attacker could send a specially crafted packet to an affected DHCP server. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. The security update addresses the vulnerability by correcting how DHCP servers initializes memory.	7.5	More Details
CVE-2020-2041	An insecure configuration of the appweb daemon of Palo Alto Networks PAN-OS 8.1 allows a remote unauthenticated user to send a specifically crafted request to the device that causes the appweb service to crash. 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 all versions of PAN-OS 8.0, and PAN-OS 8.1 versions earlier than 8.1.16.	7.5	More Details
CVE-2020-25540	ThinkAdmin v6 is affected by a directory traversal vulnerability. An unauthorized attacker can read arbitrarily file on a remote server via GET request encode parameter.	7.5	More Details
CVE-2020-25281	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. Applications with sensitive security settings (such as the package verifier application) mishandle unknown-source installations. The LG ID is LVE-SMP-190002 (September 2020).	7.5	More Details
CVE-2020-1045	A security feature bypass vulnerability exists in the way Microsoft ASP.NET Core parses encoded cookie names. The ASP.NET Core cookie parser decodes entire cookie strings which could allow a malicious attacker to set a second cookie with the name being percent encoded. The security update addresses the vulnerability by fixing the way the ASP.NET Core cookie parser handles encoded names.	7.5	More Details
CVE-2020-25219	url::recvline in url.cpp in libproxy 0.4.x through 0.4.15 allows a remote HTTP server to trigger uncontrolled recursion via a response composed of an infinite stream that lacks a newline character. This leads to stack exhaustion.	7.5	More Details
CVE-2020-12787	Microchip Atmel ATSAMA5 products in Secure Mode allow an attacker to bypass existing security mechanisms related to applet handling.	7.5	More Details
CVE-2020-12788	CMAC verification functionality in Microchip Atmel ATSAMA5 products is vulnerable to vulnerable to timing and power analysis attacks.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1198	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. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	7.4	More Details
CVE-2020-1345	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. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	7.4	More Details
CVE-2020-10049	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.10.2). The start-stop scripts for the services of the affected application could allow a local attacker to include arbitrary commands that are executed when services are started or stopped interactively by system administrators.	7.3	More Details
CVE-2020-0570	Uncontrolled search path in the QT Library before 5.14.0, 5.12.7 and 5.9.10 may allow an authenticated user to potentially enable elevation of privilege via local access.	7.3	More Details
CVE-2020-1319	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Exploitation of the vulnerability requires that a program process a specially crafted image file. The update addresses the vulnerability by correcting how Microsoft Windows Codecs Library handles objects in memory.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25276	An issue was discovered in PrimeKey EJBCA 6.x and 7.x before 7.4.1. When using a client certificate to enroll over the EST protocol, no revocation check is performed on that certificate. This vulnerability can only affect a system that has EST configured, uses client certificates to authenticate enrollment, and has had such a certificate revoked. This certificate needs to belong to a role that is authorized to enroll new end entities. (To completely mitigate this problem prior to upgrade, remove any revoked client certificates from their respective roles.)	7.3	More Details
CVE-2020-1471	An elevation of privilege vulnerability exists when Microsoft Windows CloudExperienceHost fails to check COM objects. An attacker who successfully exploited the vulnerability could gain elevated privileges on a targeted system. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application. The security update addresses the vulnerability by checking COM objects.	7.3	More Details
CVE-2020-8342	A race condition vulnerability was reported in Lenovo System Update prior to version 5.07.0106 that could allow escalation of privilege.	7.3	More Details
CVE-2020-16097	On controllers running versions of v8.20 prior to vCR8.20.200221b (distributed in v8.20.1093(MR2)), v8.10 prior to vGR8.10.179 (distributed in v8.10.1211(MR5)), v8.00 prior to vGR8.00.165 (Distributed in v8.00.1228(MR6)), v7.90 prior to vGR7.90.165 (distributed in v7.90.1038(MRX)), v7.80 or earlier, It is possible to retrieve site keys used for securing MIFARE Plus and Desfire using debug ports on T Series readers.	7.3	More Details
CVE-2020-25287	Pligg 2.0.3 allows remote authenticated users to execute arbitrary commands because the template editor can edit any file, as demonstrated by an admin/admin_editor.php the_file=..%2Findex.php&open=Open request.	7.2	More Details
CVE-2020-6318	A Remote Code Execution vulnerability exists in the SAP NetWeaver (ABAP Server, up to release 7.40) and ABAP Platform (> release 7.40).Because of this, an attacker can exploit these products via Code Injection, and potentially enabling to take complete control of the products, including viewing, changing, or deleting data by injecting code into the working memory which is subsequently executed by the application. It can also be used to cause a general fault in the product, causing the products to terminate.	7.2	More Details
CVE-2020-11977	In Apache Syncope 2.1.X releases prior to 2.1.7, when the Flowable extension is enabled, an administrator with workflow entitlements can use Shell Service Tasks to perform malicious operations, including but not limited to file read, file write, and code execution.	7.2	More Details
CVE-2020-2038	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 9.0 versions earlier than 9.0.10; PAN-OS 9.1 versions earlier than 9.1.4; PAN-OS 10.0 versions earlier than 10.0.1.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13298	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Conan package upload functionality was not properly validating the supplied parameters, which resulted in the limited files disclosure.	7.2	More Details
CVE-2020-2042	A buffer overflow vulnerability in the PAN-OS management web interface allows authenticated administrators to disrupt system processes and potentially execute arbitrary code with root privileges. This issue impacts only PAN-OS 10.0 versions earlier than PAN-OS 10.0.1.	7.2	More Details
CVE-2020-2037	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 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.3.	7.2	More Details
CVE-2020-16852	An elevation of privilege vulnerability exists when the OneDrive for Windows Desktop application improperly handles symbolic links. An attacker who successfully exploited this vulnerability could overwrite a targeted file with an elevated status. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and delete a targeted file with an elevated status. The update addresses this vulnerability by correcting where the OneDrive updater performs file writes while running with elevation.	7.1	More Details
CVE-2020-16853	An elevation of privilege vulnerability exists when the OneDrive for Windows Desktop application improperly handles symbolic links. An attacker who successfully exploited this vulnerability could overwrite a targeted file with an elevated status. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and delete a targeted file with an elevated status. The update addresses this vulnerability by correcting where the OneDrive updater performs file writes while running with elevation.	7.1	More Details
CVE-2020-16862	A remote code execution vulnerability exists in Microsoft Dynamics 365 (on-premises) when the server fails to properly sanitize web requests to an affected Dynamics server. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SQL service account. An authenticated attacker could exploit this vulnerability by sending a specially crafted request to a vulnerable Dynamics server. The security update addresses the vulnerability by correcting how Microsoft Dynamics 365 (on-premises) validates and sanitizes user input.	7.1	More Details
CVE-2020-16851	An elevation of privilege vulnerability exists when the OneDrive for Windows Desktop application improperly handles symbolic links. An attacker who successfully exploited this vulnerability could overwrite a targeted file with an elevated status. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and delete a targeted file with an elevated status. The update addresses this vulnerability by correcting where the OneDrive updater performs file writes while running with elevation.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16857	A remote code execution vulnerability exists in Microsoft Dynamics 365 for Finance and Operations (on-premises) version 10.0.11. An attacker who successfully exploited this vulnerability could gain remote code execution via server-side script execution on the victim server. An authenticated attacker with privileges to import and export data could exploit this vulnerability by sending a specially crafted file to a vulnerable Dynamics server. The security update addresses the vulnerability by correcting how Microsoft Dynamics 365 for Finance and Operations (on-premises) version 10.0.11 handles user input.	7.1	More Details
CVE-2020-3617	u'Buffer over-read Issue in Q6 testbus framework due to diag packet length is not completely validated before accessing the field and leads to Information disclosure.' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Kamorta, Nicobar, QCS605, QCS610, Rennell, SC7180, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SXR1130	7.1	More Details
CVE-2020-13303	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Due to improper verification of permissions, an unauthorized user can access a private repository within a public project.	7.1	More Details
CVE-2020-1245	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how Win32k handles objects in memory.	7.0	More Details
CVE-2020-15170	apollo-adminservice before version 1.7.1 does not implement access controls. If users expose apollo-adminservice to internet(which is not recommended), there are potential security issues since apollo-adminservice is designed to work in intranet and it doesn't have access control built-in. Malicious hackers may access apollo-adminservice apis directly to access/edit the application's configurations. To fix the potential issue without upgrading, simply follow the advice that do not expose apollo-adminservice to internet.	7.0	More Details
CVE-2020-1308	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how DirectX handles objects in memory.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0912	An elevation of privilege vulnerability exists when the Windows Function Discovery SSDP Provider improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Windows Function Discovery SSDP Provider handles memory.	7.0	More Details
CVE-2020-25212	A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt memory or possibly have unspecified other impact because a size check is in fs/nfs/nfs4proc.c instead of fs/nfs/nfs4xdr.c, aka CID-b4487b935452.	7.0	More Details
CVE-2020-7323	Authentication Protection Bypass vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows physical local users to bypass the Windows lock screen via triggering certain detection events while the computer screen is locked and the McTray.exe is running with elevated privileges. This issue is timing dependent and requires physical access to the machine.	6.9	More Details
CVE-2020-16212	In Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, the product exposes a resource to the wrong control sphere, providing unintended actors with inappropriate access to the resource. The application on the surveillance station operates in kiosk mode, which is vulnerable to local breakouts that could allow an attacker with physical access to escape the restricted environment with limited privileges.	6.8	More Details
CVE-2020-16860	A remote code execution vulnerability exists in Microsoft Dynamics 365 (on-premises) when the server fails to properly sanitize web requests to an affected Dynamics server. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SQL service account. An authenticated attacker could exploit this vulnerability by sending a specially crafted request to a vulnerable Dynamics server. The security update addresses the vulnerability by correcting how Microsoft Dynamics 365 (on-premises) validates and sanitizes user input.	6.8	More Details
CVE-2020-1034	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.	6.8	More Details
CVE-2018-17774	Ingenico Telium 2 POS terminals have an insecure NTPT3 protocol. This is fixed in Telium 2 SDK v9.32.03 patch N.	6.8	More Details
CVE-2018-17767	Ingenico Telium 2 POS terminals have hardcoded PPP credentials. This is fixed in Telium 2 SDK v9.32.03 patch N.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-17768	Ingenico Telium 2 POS terminals have an insecure TRACE protocol. This is fixed in Telium 2 SDK v9.32.03 patch N.	6.8	More Details
CVE-2020-9738	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by a stored XSS vulnerability that allows users with access to the Content Repository Development Environment to store malicious scripts in certain node fields. These scripts may be executed in a victim's browser when visiting the page containing the vulnerable field.	6.8	More Details
CVE-2020-9735	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by a stored XSS vulnerability that allows users with access to the Content Repository Development Environment to store malicious scripts in certain node fields. These scripts may be executed in a victim's browser when search queries return the page containing the vulnerable field.	6.8	More Details
CVE-2020-25280	An issue was discovered on Samsung mobile devices with Q(10.0) (Exynos and MediaTek chipsets) software. Unauthenticated attackers can execute LTE/5G commands by sending a debugging command over USB. The Samsung ID is SVE-2020-16979 (September 2020).	6.8	More Details
CVE-2018-17765	Ingenico Telium 2 POS terminals have undeclared TRACE protocol commands. This is fixed in Telium 2 SDK v9.32.03 patch N.	6.8	More Details
CVE-2020-9736	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by a stored XSS vulnerability that allows users with access to the Content Repository Development Environment to store malicious scripts in certain node fields. These scripts may be executed in a victim's browser when browsing to the page containing the vulnerable field.	6.8	More Details
CVE-2020-9737	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by a stored XSS vulnerability that allows users with access to the Content Repository Development Environment to store malicious scripts in certain node fields. These scripts may be executed in a victim's browser when they open the page containing the vulnerable field.	6.8	More Details
CVE-2020-11683	A timing side channel was discovered in AT91bootstrap before 3.9.2. It can be exploited by attackers with physical access to forge CMAC values and subsequently boot arbitrary code on an affected system.	6.8	More Details
CVE-2018-17772	Ingenico Telium 2 POS terminals allow arbitrary code execution via the TRACE protocol. This is fixed in Telium 2 SDK v9.32.03 patch N.	6.8	More Details
CVE-2018-17773	Ingenico Telium 2 POS terminals have a buffer overflow via SOCKET_TASK in the NTPT3 protocol. This is fixed in Telium 2 SDK v9.32.03 patch N.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7320	Protection Mechanism Failure vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local administrator to temporarily reduce the detection capability allowing otherwise detected malware to run via stopping certain Microsoft services.	6.7	More Details
CVE-2020-0951	A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement. An attacker who successfully exploited this vulnerability could execute PowerShell commands that would be blocked by WDAC. To exploit the vulnerability, an attacker need administrator access on a local machine where PowerShell is running. The attacker could then connect to a PowerShell session and send commands to execute arbitrary code. The update addresses the vulnerability by correcting how PowerShell commands are validated when WDAC protection is enabled.	6.7	More Details
CVE-2018-17769	Ingenico Telium 2 POS terminals have a buffer overflow via the 0x26 command of the NTPT3 protocol. This is fixed in Telium 2 SDK v9.32.03 patch N.	6.6	More Details
CVE-2018-17770	Ingenico Telium 2 POS terminals have a buffer overflow via the RemotePutFile command of the NTPT3 protocol. This is fixed in Telium 2 SDK v9.32.03 patch N.	6.6	More Details
CVE-2018-17771	Ingenico Telium 2 POS terminals have hardcoded FTP credentials. This is fixed in Telium 2 SDK v9.32.03 patch N.	6.6	More Details
CVE-2020-1130	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector improperly handles data operations. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Diagnostics Hub Standard Collector handles data operations.	6.6	More Details
CVE-2020-1146	An elevation of privilege vulnerability exists when the Microsoft Store Runtime improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Microsoft Store Runtime handles memory.	6.6	More Details
CVE-2020-14331	A flaw was found in the Linux kernel's implementation of the invert video code on VGA consoles when a local attacker attempts to resize the console, calling an ioctl VT_RESIZE, which causes an out-of-bounds write to occur. This flaw allows a local user with access to the VGA console to crash the system, potentially escalating their privileges on the system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1590	An elevation of privilege vulnerability exists when the Connected User Experiences and Telemetry Service improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges on the victim system. To exploit the vulnerability, an attacker would first have to gain execution on the victim system, then run a specially crafted application. The security update addresses the vulnerability by correcting how the Connected User Experiences and Telemetry Service handles file operations.	6.6	More Details
CVE-2020-15171	In XWiki before versions 11.10.5 or 12.2.1, any user with SCRIPT right (EDIT right before XWiki 7.4) can gain access to the application server Servlet context which contains tools allowing to instantiate arbitrary Java objects and invoke methods that may lead to arbitrary code execution. The only workaround is to give SCRIPT right only to trusted users.	6.6	More Details
CVE-2020-1159	An elevation of privilege vulnerability exists in the way that the StartTileData.dll handles file creation in protected locations. 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 StartTileData.dll properly handles this type of function.	6.6	More Details
CVE-2020-16216	In IntelliVue patient monitors MX100, MX400-550, MX600, MX700, MX750, MX800, MX850, MP2-MP90, and IntelliVue X2 and X3 Versions N and prior, the product receives input or data but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly, which can induce a denial-of-service condition through a system restart.	6.5	More Details
CVE-2020-0856	An information disclosure vulnerability exists when Active Directory integrated DNS (ADIDNS) mishandles objects in memory. An authenticated attacker who successfully exploited this vulnerability would be able to read sensitive information about the target system. To exploit this condition, an authenticated attacker would need to send a specially crafted request to the ADIDNS service. Note that the information disclosure vulnerability by itself would not be sufficient for an attacker to compromise a system. However, an attacker could combine this vulnerability with additional vulnerabilities to further exploit the system. The update addresses the vulnerability by correcting how Active Directory integrated DNS (ADIDNS) handles objects in memory.	6.5	More Details
CVE-2020-1097	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise a user's system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document or by convincing a user to visit an untrusted webpage. The update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1091	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise a user's system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document or by convincing a user to visit an untrusted webpage. The update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory.	6.5	More Details
CVE-2020-6313	SAP NetWeaver Application Server JAVA(XML Forms) versions 7.30, 7.31, 7.40, 7.50 does not sufficiently encode user controlled inputs, which allows an authenticated User with special roles to store malicious content, that when accessed by a victim, can perform malicious actions by executing JavaScript, leading to Stored Cross-Site Scripting.	6.5	More Details
CVE-2020-13312	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab OAuth endpoint was vulnerable to brute-force attacks through a specific parameter.	6.5	More Details
CVE-2020-6321	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated U3D file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	6.5	More Details
CVE-2020-16224	In Patient Information Center iX (PICiX) Versions C.02, C.03, the software parses a formatted message or structure but does not handle or incorrectly handles a length field that is inconsistent with the actual length of the associated data, causing the application on the surveillance station to restart.	6.5	More Details
CVE-2020-15791	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 CPU family (incl. SIPLUS variants) (All versions), SIMATIC WinAC RTX (F) 2010 (All versions), SINUMERIK 840D sl (All versions). The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials.	6.5	More Details
CVE-2020-13317	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8, and 13.3.4. An insufficient check in the GraphQL api allowed a maintainer to delete a repository.	6.5	More Details
CVE-2020-0904	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application. The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4711	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 187501.	6.5	More Details
CVE-2020-0890	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application. The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests.	6.5	More Details
CVE-2019-20918	An issue was discovered in InspIRCd 3 before 3.1.0. The silence module contains a use after free vulnerability. This vulnerability can be used for remote crashing of an InspIRCd server by any user able to fully connect to a server.	6.5	More Details
CVE-2020-0664	An information disclosure vulnerability exists when Active Directory integrated DNS (ADIDNS) mishandles objects in memory. An authenticated attacker who successfully exploited this vulnerability would be able to read sensitive information about the target system. To exploit this condition, an authenticated attacker would need to send a specially crafted request to the ADIDNS service. Note that the information disclosure vulnerability by itself would not be sufficient for an attacker to compromise a system. However, an attacker could combine this vulnerability with additional vulnerabilities to further exploit the system. The update addresses the vulnerability by correcting how Active Directory integrated DNS (ADIDNS) handles objects in memory.	6.5	More Details
CVE-2020-6311	Banking services from SAP 9.0 (Bank Analyzer), version - 500, and SAP S/4HANA for financial products subledger, version 100, does not correctly perform necessary authorization checks for an authenticated user due to Improper Authorization checks, that may cause a system administrator to create incorrect authorization proposals. This may result in privilege escalation and may expose restricted banking data.	6.5	More Details
CVE-2019-20917	An issue was discovered in InspIRCd 2 before 2.0.28 and 3 before 3.3.0. The mysql module contains a NULL pointer dereference when built against mariadb-connector-c 3.0.5 or newer. When combined with the sqlauth or sqloper modules, this vulnerability can be used for remote crashing of an InspIRCd server by any user able to connect to a server.	6.5	More Details
CVE-2020-24739	A CSRF vulnerability was found in iCMS v7.0.0 in the background deletion administrator account. When missing the CSRF_TOKEN and can still request normally, all administrators except the initial administrator will be deleted.	6.5	More Details
CVE-2020-13284	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. API Authorization Using Outdated CI Job Token	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13310	A vulnerability was discovered in GitLab runner versions before 13.1.3, 13.2.3 and 13.3.1. It was possible to make the gitlab-runner process crash by sending malformed queries, resulting in a denial of service.	6.5	More Details
CVE-2020-25269	An issue was discovered in InspIRCd 2 before 2.0.29 and 3 before 3.6.0. The pgsql module contains a use after free vulnerability. When combined with the sqlauth or sqloper modules, this vulnerability can be used for remote crashing of an InspIRCd server by any user able to connect to a server.	6.5	More Details
CVE-2020-25285	A race condition between hugetlb sysctl handlers in mm/hugetlb.c in the Linux kernel before 5.8.8 could be used by local attackers to corrupt memory, cause a NULL pointer dereference, or possibly have unspecified other impact, aka CID-17743798d812.	6.4	More Details
CVE-2020-13318	A vulnerability was discovered in GitLab versions before 13.0.12, 13.1.10, 13.2.8 and 13.3.4. GitLabs EKS integration was vulnerable to a cross-account assume role attack.	6.4	More Details
CVE-2020-16228	In Patient Information Center iX (PICiX) Versions C.02 and C.03, PerformanceBridge Focal Point Version A.01, IntelliVue patient monitors MX100, MX400-MX550, MX750, MX850, and IntelliVue X3 Versions N and prior, the software does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a compromised certificate.	6.4	More Details
CVE-2020-1482	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. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	6.3	More Details
CVE-2019-4671	IBM Maximo Asset Management 7.6.0 and 7.6.1 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 171437.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8340	A cross-site scripting (XSS) vulnerability was discovered in the legacy IBM and Lenovo System x IMM2 (Integrated Management Module 2), prior to version 5.60, embedded Baseboard Management Controller (BMC) web interface during an internal security review. This vulnerability could allow JavaScript code to be executed in the user's web browser if the user is convinced to visit a crafted URL, possibly through phishing. Successful exploitation requires specific knowledge about the user’s network to be included in the crafted URL. Impact is limited to the normal access restrictions and permissions of the user clicking the crafted URL, and subject to the user being able to connect to and already being authenticated to IMM2 or other systems. The JavaScript code is not executed on IMM2 itself.	6.3	More Details
CVE-2020-1440	A tampering vulnerability exists when Microsoft SharePoint Server fails to properly handle profile data. An attacker who successfully exploited this vulnerability could modify a targeted user's profile data. To exploit the vulnerability, an attacker would need to be authenticated on an affected SharePoint Server. The attacker would then need to send a specially modified request to the server, targeting a specific user. The security update addresses the vulnerability by modifying how Microsoft SharePoint Server handles profile data.	6.3	More Details
CVE-2020-7324	Improper Access Control vulnerability in McAfee MVISION Endpoint prior to 20.9 Update allows local users to bypass security mechanisms and deny access to the SYSTEM folder via incorrectly applied permissions.	6.1	More Details
CVE-2019-14758	An issue was discovered in KaiOS 2.5 and 2.5.1. The pre-installed File Manager application is vulnerable to HTML and JavaScript injection attacks. An attacker can send a file via email to the victim that will inject HTML into the File Manager application (assuming the victim chooses to download the email attachment). At a bare minimum, this allows an attacker to take control over the File Manager application's UI (e.g., display a malicious prompt to the user asking them to re-enter credentials such as their KaiOS credentials to continue using the application) and also allows an attacker to abuse any of the privileges available to the mobile application.	6.1	More Details
CVE-2019-14756	An issue was discovered in KaiOS 1.0, 2.5, and 2.5.12.5. The pre-installed Email application is vulnerable to HTML and JavaScript injection attacks. An attacker can send a specially crafted email to the victim that will inject HTML into the email application's UI as soon as the email is opened. At a bare minimum, this allows an attacker to take control over the Email application's UI (e.g., display a malicious prompt to the user asking them to re-enter their email credentials) and also allows an attacker to abuse any of the privileges available to the mobile application.	6.1	More Details
CVE-2020-10227	A cross-site scripting (XSS) vulnerability in the messages module of vtecrm vtenext 19 CE allows attackers to inject arbitrary JavaScript code via the From field of an email.	6.1	More Details
CVE-2020-21845	Codoforum 4.8.3 allows HTML Injection in the 'admin dashboard Manage users Section.'	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15788	A vulnerability has been identified in Polarion Subversion Webclient (All versions). The Polarion subversion web application does not filter user input in a way that prevents Cross-Site Scripting. If a user is enticed into passing specially crafted, malicious input to the web client (e.g. by clicking on a malicious URL with embedded JavaScript), then JavaScript code can be returned and may then be executed by the user's client. Various actions could be triggered by running malicious JavaScript code.	6.1	More Details
CVE-2020-21733	Sagemcom F@ST3686 v1.0 HUN 3.97.0 has XSS via RgDiagnostics.asp, RgDdns.asp, RgFirewallEL.asp, RgVpnL2tpPptp.asp.	6.1	More Details
CVE-2020-6283	SAP Fiori Launchpad does not sufficiently encode user controlled inputs, and hence allowing the attacker to inject the meta tag into the launchpad html using the vulnerable parameter, resulting in reflected Cross-Site Scripting (XSS) vulnerability. With a successful attack, the attacker can steal authentication information of the user, such as data relating to his or her current session.	6.1	More Details
CVE-2020-5627	Yodobashi App for Android versions 1.8.7 and earlier allows remote attackers to lead a user to access an arbitrary website via the vulnerable App. As a result, the user may become a victim of a phishing attack.	6.1	More Details
CVE-2020-21732	Rukovoditel Project Management app 2.6 is affected by: Cross Site Scripting (XSS). An attacker can add JavaScript code to the filename.	6.1	More Details
CVE-2020-24194	A Cross-site scripting (XSS) vulnerability in 'user-profile.php' in SourceCodester Daily Tracker System v1.0 allows remote attackers to inject arbitrary web script or HTML via the 'fullname' parameter.	6.1	More Details
CVE-2020-21731	Gazie 7.29 is affected by: Cross Site Scripting (XSS) via http://192.168.100.7/gazie/modules/config/admin_utente.php?user_name=amministratore&Update. An attacker can inject JavaScript code, and the webapplication stores the injected code.	6.1	More Details
CVE-2020-9726	Adobe FrameMaker version 2019.0.6 (and earlier versions) has an out-of-bounds read vulnerability that could be exploited to read past the end of an allocated buffer, possibly resulting in a crash or disclosure of sensitive information from other memory locations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious FrameMaker file.	6.1	More Details
CVE-2020-24582	Zulip Desktop before 5.4.3 allows XSS because string escaping is mishandled during composition of the HTML for the user interface.	6.1	More Details
CVE-2020-6324	SAP Netweaver AS ABAP(BSP Test Application sbspext_table), version-700,701,720,730,731,740,750,751,752,753,754,755, allows an unauthenticated attacker to send polluted URL to the victim, when the victim clicks on this URL, the attacker can read, modify the information available in the victim's browser leading to Reflected Cross Site Scripting.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24198	A persistent cross-site scripting vulnerability in Sourcecodester Stock Management System v1.0 allows remote attackers to inject arbitrary web script or HTML via the 'Brand Name.'	6.1	More Details
CVE-2020-24794	Cross Site Scripting (XSS) vulnerability in Kentico before 12.0.75.	6.1	More Details
CVE-2020-1506	An elevation of privilege vulnerability exists in the way that the Wininit.dll handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. There are multiple ways an attacker could exploit the vulnerability: - In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. - In a file sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit this vulnerability, and then convince a user to open the document file. The security update addresses the vulnerability by ensuring the Wininit.dll properly handles objects in memory.	6.1	More Details
CVE-2020-25378	Wordpress Plugin Store / AccessPress Themes WP Floating Menu V1.3.0 is affected by: Cross Site Scripting (XSS) via the id GET parameter.	6.1	More Details
CVE-2019-14757	An issue was discovered in KaiOS 2.5 and 2.5.1. The pre-installed Contacts application is vulnerable to HTML and JavaScript injection attacks. An attacker can send a vCard file to the victim that will inject HTML into the Contacts application (assuming the victim chooses to import the file). At a bare minimum, this allows an attacker to take control over the Contacts application's UI (e.g., display a malicious prompt to the user asking them to re-enter credentials such as their KaiOS credentials to continue using the application) and also allows an attacker to abuse any of the privileges available to the mobile application.	6.1	More Details
CVE-2020-1598	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application. The update addresses the vulnerability by correcting how the Windows UPnP service handles objects in memory.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22158	MediaKind (formerly Ericsson) RX8200 5.13.3 devices are vulnerable to multiple reflected and stored XSS. An attacker has to inject JavaScript code directly in the "path" or "Services+ID" parameters and send the URL to a user in order to exploit reflected XSS. In the case of stored XSS, an attacker must modify the "name" parameter with the malicious code.	6.1	More Details
CVE-2014-10401	An issue was discovered in the DBI module before 1.632 for Perl. DBD::File drivers can open files from folders other than those specifically passed via the f_dir attribute.	6.1	More Details
CVE-2020-25211	In the Linux kernel through 5.8.7, local attackers able to inject conntrack netlink configuration could overflow a local buffer, causing crashes or triggering use of incorrect protocol numbers in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c, aka CID-1cc5ef91d2ff.	6.0	More Details
CVE-2020-7315	DLL Injection Vulnerability in McAfee Agent (MA) for Windows prior to 5.6.6 allows local users to execute arbitrary code via careful placement of a malicious DLL.	6.0	More Details
CVE-2020-10759	A PGP signature bypass flaw was found in fwupd (all versions), which could lead to the installation of unsigned firmware. As per upstream, a signature bypass is theoretically possible, but not practical because the Linux Vendor Firmware Service (LVFS) is either not implemented or enabled in versions of fwupd shipped with Red Hat Enterprise Linux 7 and 8. The highest threat from this vulnerability is to confidentiality and integrity.	6.0	More Details
CVE-2020-13920	Apache ActiveMQ uses LocateRegistry.createRegistry() to create the JMX RMI registry and binds the server to the "jmxrmi" entry. It is possible to connect to the registry without authentication and call the rebind method to rebind jmxrmi to something else. If an attacker creates another server to proxy the original, and bound that, he effectively becomes a man in the middle and is able to intercept the credentials when an user connects. Upgrade to Apache ActiveMQ 5.15.12.	5.9	More Details
CVE-2020-15802	Devices supporting Bluetooth before 5.1 may allow man-in-the-middle attacks, aka BLURtooth. Cross Transport Key Derivation in Bluetooth Core Specification v4.2 and v5.0 may permit an unauthenticated user to establish a bonding with one transport, either LE or BR/EDR, and replace a bonding already established on the opposing transport, BR/EDR or LE, potentially overwriting an authenticated key with an unauthenticated key, or a key with greater entropy with one with less.	5.9	More Details
CVE-2020-1152	An elevation of privilege vulnerability exists when Windows improperly handles calls to Win32k.sys. An attacker who successfully exploited the vulnerability could gain elevated privileges on a targeted system. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application. The update addresses the vulnerability by correcting how Windows handles calls to Win32k.	5.8	More Details
CVE-2020-7296	Privilege Escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows authenticated user interface user to access protected configuration files via improper access control in the user interface.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14292	In the COVIDSafe application through 1.0.21 for Android, unsafe use of the Bluetooth transport option in the GATT connection allows attackers to trick the application into establishing a connection over Bluetooth BR/EDR transport, which reveals the public Bluetooth address of the victim's phone without authorisation, bypassing the Bluetooth address randomisation protection in the user's phone.	5.7	More Details
CVE-2020-7807	A vulnerability that can hijack a DLL file that is loaded during products(LGPCSuite_Setup, IPSFULLHD, LG_ULTRAWIDE, ULTRA_HD_Driver Setup) installation into a DLL file that the hacker wants. Missing Support for Integrity Check vulnerability in ____COMPONENT____ of LG Electronics (LGPCSuite_Setup), (IPSFULLHD, LG_ULTRAWIDE, ULTRA_HD_Driver Setup) allows ____ATTACKER/ATTACK____ to cause ____IMPACT____. This issue affects: LG Electronics; LGPCSuite_Setup : 1.0.0.3 on Windows(x86, x64); IPSFULLHD, LG_ULTRAWIDE, ULTRA_HD_Driver Setup : 1.0.0.9 on Windows(x86, x64).	5.6	More Details
CVE-2020-0914	An information disclosure vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user’s system. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory.	5.5	More Details
CVE-2020-1250	An information disclosure vulnerability exists when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user’s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how win32k handles objects in memory.	5.5	More Details
CVE-2020-0921	Microsoft Graphics Component Denial of Service Vulnerability	5.5	More Details
CVE-2020-14385	A flaw was found in the Linux kernel before 5.9-rc4. A failure of the file system metadata validator in XFS can cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt. This can lead to the filesystem being shutdown, or otherwise rendered inaccessible until it is remounted, leading to a denial of service. The highest threat from this vulnerability is to system availability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0875	An information disclosure vulnerability exists in how splwow64.exe handles certain calls. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system (low-integrity to medium-integrity). This vulnerability by itself does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability (such as a remote code execution vulnerability or another elevation of privilege vulnerability) that is capable of leveraging the elevated privileges when code execution is attempted. The security update addresses the vulnerability by ensuring splwow64.exe properly handles these calls.	5.5	More Details
CVE-2020-14314	A memory out-of-bounds read flaw was found in the Linux kernel before 5.9-rc2 with the ext3/ext4 file system, in the way it accesses a directory with broken indexing. This flaw allows a local user to crash the system if the directory exists. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2020-3679	u'During execution after Address Space Layout Randomization is turned on for QTEE, part of code is still mapped at known address including code segments' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Bitra, Kamorta, Nicobar, QCS404, QCS610, Rennell, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	5.5	More Details
CVE-2020-7325	Privilege Escalation vulnerability in McAfee MVISION Endpoint prior to 20.9 Update allows local users to access files which the user otherwise would not have access to via manipulating symbolic links to redirect McAfee file operations to an unintended file.	5.5	More Details
CVE-2020-8346	A denial of service vulnerability was reported in the Lenovo Vantage component called Lenovo System Interface Foundation prior to version 1.1.19.5 that could allow configuration files to be written to non-standard locations.	5.5	More Details
CVE-2020-9239	Huawei smartphones BLA-A09 versions 8.0.0.123(C212),versions earlier than 8.0.0.123(C567),versions earlier than 8.0.0.123(C797);BLA-TL00B versions earlier than 8.1.0.326(C01);Berkeley-L09 versions earlier than 8.0.0.163(C10),versions earlier than 8.0.0.163(C432),Versions earlier than 8.0.0.163(C636),Versions earlier than 8.0.0.172(C10);Duke-L09 versions Duke-L09C10B187, versions Duke-L09C432B189, versions Duke-L09C636B189;HUAWEI P20 versions earlier than 8.0.1.16(C00);HUAWEI P20 Pro versions earlier than 8.1.0.152(C00);Jimmy-AL00A versions earlier than Jimmy-AL00AC00B172;LON-L29D versions LON-L29DC721B192;NEO-AL00D versions earlier than 8.1.0.172(C786);Stanford-AL00 versions Stanford-AL00C00B123;Toronto-AL00 versions earlier than Toronto-AL00AC00B225;Toronto-AL00A versions earlier than Toronto-AL00AC00B225;Toronto-TL10 versions earlier than Toronto-TL10C01B225 have an information vulnerability. A module has a design error that is lack of control of input. Attackers can exploit this vulnerab	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1133	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector improperly handles file operations. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Diagnostics Hub Standard Collector handles file operations.	5.5	More Details
CVE-2020-1256	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory.	5.5	More Details
CVE-2020-1303	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory.	5.5	More Details
CVE-2020-13301	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was vulnerable to a stored XSS on the standalone vulnerability page.	5.5	More Details
CVE-2020-15024	An issue was discovered in the Login Password feature of the Password Manager component in Avast Antivirus 20.1.5069.562. An entered password continues to be stored in Windows main memory after a logout, and after a Lock Vault operation.	5.5	More Details
CVE-2020-24552	Atop Technology industrial 3G/4G gateway contains Command Injection vulnerability. Due to insufficient input validation, the device's web management interface allows attackers to inject specific code and execute system commands without privilege.	5.5	More Details
CVE-2020-25289	The VPN service in AVAST SecureLine before 5.6.4982.470 allows local users to write to arbitrary files via an Object Manager symbolic link from the log directory (which has weak permissions).	5.5	More Details
CVE-2020-0928	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1224	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the user's computer or data. To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created. The update addresses the vulnerability by changing the way certain Excel functions handle objects in memory.	5.5	More Details
CVE-2020-0941	An information disclosure vulnerability exists when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability, an attacker would have to either log on locally to an affected system, or convince a locally authenticated user to execute a specially crafted application. The security update addresses the vulnerability by correcting how win32k handles objects in memory.	5.5	More Details
CVE-2020-1083	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The update addresses the vulnerability by correcting the way in which the Windows Graphics Component handles objects in memory.	5.5	More Details
CVE-2020-16879	An information disclosure vulnerability exists when a Windows Projected Filesystem improperly handles file redirections. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability. The security update addresses the vulnerability by correcting how Windows Projected Filesystem handle file redirections.	5.5	More Details
CVE-2020-1038	A denial of service vulnerability exists when Windows Routing Utilities improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to cause a target system to stop responding. The update addresses the vulnerability by correcting how Windows handles objects in memory.	5.5	More Details
CVE-2020-10767	A flaw was found in the Linux kernel before 5.8-rc1 in the implementation of the Enhanced IBPB (Indirect Branch Prediction Barrier). The IBPB mitigation will be disabled when STIBP is not available or when the Enhanced Indirect Branch Restricted Speculation (IBRS) is available. This flaw allows a local attacker to perform a Spectre V2 style attack when this configuration is active. The highest threat from this vulnerability is to confidentiality.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10766	A logic bug flaw was found in Linux kernel before 5.8-rc1 in the implementation of SSBD. A bug in the logic handling allows an attacker with a local account to disable SSBD protection during a context switch when additional speculative execution mitigations are in place. This issue was introduced when the per task/process conditional STIPB switching was added on top of the existing SSBD switching. The highest threat from this vulnerability is to confidentiality.	5.5	More Details
CVE-2020-0989	An information disclosure vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions. An attacker who successfully exploited this vulnerability could bypass access restrictions to read files. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and access files. The security update addresses the vulnerability by correcting the how Windows MDM Diagnostics handles files.	5.5	More Details
CVE-2020-3674	Information can leak into userspace due to improper transfer of data from kernel to userspace in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in Nicobar, QCS405, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130	5.5	More Details
CVE-2020-14332	A flaw was found in the Ansible Engine when using module_args. Tasks executed with check mode (--check-mode) do not properly neutralize sensitive data exposed in the event data. This flaw allows unauthorized users to read this data. The highest threat from this vulnerability is to confidentiality.	5.5	More Details
CVE-2020-1122	An elevation of privilege vulnerability exists when the Windows Language Pack Installer improperly handles file operations. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Language Pack Installer handles file operations.	5.5	More Details
CVE-2020-1119	An information disclosure vulnerability exists when StartTileData.dll improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The update addresses the vulnerability by correcting the way in which StartTileData.dll handles objects in memory.	5.5	More Details
CVE-2020-16854	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16855	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. An attacker who successfully exploited the vulnerability could view out of bound memory. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. The security update addresses the vulnerability by properly initializing the affected variable.	5.5	More Details
CVE-2020-6312	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), versions - 4.1, 4.2, allows an attacker with a non-administrative user account that can edit certain web page properties, can modify how a browser processes particular page elements, leading to stored Cross Site Scripting. In certain situations, when a user accesses an affected web page element, the attacker will be able to access or modify metadata for which they are not authorized.	5.4	More Details
CVE-2020-16871	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	5.4	More Details
CVE-2020-1575	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. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1514	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. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	5.4	More Details
CVE-2020-16878	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	5.4	More Details
CVE-2020-25375	Wordpress Plugin Store / SoftradeWeb SNC WP SMART CRM V1.8.7 is affected by: Cross Site Scripting via the Business Name field, Tax Code field, First Name field, Address field, Town field, Phone field, Mobile field, Place of Birth field, Web Site field, VAT Number field, Last Name field, Fax field, Email field, and Skype field.	5.4	More Details
CVE-2020-25380	Wordpress Plugin Store / Mike Rooijackers Recall Products V0.8 is affected by: Cross Site Scripting (XSS) via the 'Recall Settings' field in admin.php. An attacker can inject JavaScript code that will be stored and executed.	5.4	More Details
CVE-2020-4578	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 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: 184433.	5.4	More Details
CVE-2020-6326	SAP NetWeaver (Knowledge Management), version-7.30,7.31,7.40,7.50, allows an authenticated attacker to create malicious links in the UI, when clicked by victim, will execute arbitrary java scripts thus extracting or modifying information otherwise restricted leading to Stored Cross Site Scripting.	5.4	More Details
CVE-2020-13316	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was not validating a Deploy-Token and allowed a disabled repository be accessible via a git command line.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13289	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. In certain cases an invalid username could be accepted when 2FA is activated.	5.4	More Details
CVE-2020-13309	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was vulnerable to a blind SSRF attack through the repository mirroring feature.	5.4	More Details
CVE-2020-16858	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	5.4	More Details
CVE-2020-1596	A information disclosure vulnerability exists when TLS components use weak hash algorithms. An attacker who successfully exploited this vulnerability could obtain information to further compromise a users's encrypted transmission channel. To exploit the vulnerability, an attacker would have to conduct a man-in-the-middle attack. The update addresses the vulnerability by correcting how TLS components use hash algorithms.	5.4	More Details
CVE-2020-1227	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. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	5.4	More Details
CVE-2020-25071	Nifty Project Management Web Application 2020-08-26 allows XSS, via Add Task, that is rendered upon a Project Home visit. Note: It has been argued that this is not reproducible. "The original issue was that the task would be created and an alert would be shown on the screen. Now the task would be created, but the alert won't be executed as those attributes are now stripped.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16859	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	5.4	More Details
CVE-2020-15169	In Action View before versions 5.2.4.4 and 6.0.3.3 there is a potential Cross-Site Scripting (XSS) vulnerability in Action View's translation helpers. Views that allow the user to control the default (not found) value of the `t` and `translate` helpers could be susceptible to XSS attacks. When an HTML-unsafe string is passed as the default for a missing translation key named html or ending in _html, the default string is incorrectly marked as HTML-safe and not escaped. This is patched in versions 6.0.3.3 and 5.2.4.4. A workaround without upgrading is proposed in the source advisory.	5.4	More Details
CVE-2020-16861	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	5.4	More Details
CVE-2020-4530	IBM Business Automation Workflow C.D.0 and IBM Business Process Manager 8.0, 8.5, and 8.6 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-ForceID: 182714.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16864	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	5.4	More Details
CVE-2020-24924	A Persistent Cross-site Scripting vulnerability is found in ElkarBackup v1.3.3, where an attacker can steal the user session cookie using this vulnerability present on Policies >> action >> Name Parameter	5.4	More Details
CVE-2020-2039	An uncontrolled resource consumption vulnerability in Palo Alto Networks PAN-OS allows for a remote unauthenticated user to upload temporary files through the management web interface that are not properly deleted after the request is finished. It is possible for an attacker to disrupt the availability of the management web interface by repeatedly uploading files until available disk space is exhausted. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.4; PAN-OS 10.0 versions earlier than PAN-OS 10.0.1.	5.3	More Details
CVE-2020-15785	A vulnerability has been identified in Siveillance Video Client (All versions). In environments where Windows NTLM authentication is enabled the affected client application transmits usernames to the server in cleartext. This could allow an attacker in a privileged network position to obtain valid adminstrator login names and use this information to launch further attacks.	5.3	More Details
CVE-2020-15790	A vulnerability has been identified in Spectrum Power 4 (All versions < V4.70 SP8). If configured in an insecure manner, the web server might be susceptible to a directory listing attack.	5.3	More Details
CVE-2020-6288	SAP Business Objects Business Intelligence Platform (Web Intelligence HTML interface) allows an attacker with edit document rights to upload any file (including script files) without proper file format validation leading to Unrestricted upload of file with dangerous type vulnerability. The attacker can modify some formulas and display erroneous content. The server is not affected only the current user browser session, that can easily be closed.	5.3	More Details
CVE-2020-25286	In wp-includes/comment-template.php in WordPress before 5.4.2, comments from a post or page could sometimes be seen in the latest comments even if the post or page was not public.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-7491	An issue was discovered in the DBI module before 1.628 for Perl. Stack corruption occurs when a user-defined function requires a non-trivial amount of memory and the Perl stack gets reallocated.	5.3	More Details
CVE-2013-7490	An issue was discovered in the DBI module before 1.632 for Perl. Using many arguments to methods for Callbacks may lead to memory corruption.	5.3	More Details
CVE-2020-8927	A buffer overflow exists in the Brotli library versions prior to 1.0.8 where an attacker controlling the input length of a "one-shot" decompression request to a script can trigger a crash, which happens when copying over chunks of data larger than 2 GiB. It is recommended to update your Brotli library to 1.0.8 or later. If one cannot update, we recommend to use the "streaming" API as opposed to the "one-shot" API, and impose chunk size limits.	5.3	More Details
CVE-2020-15784	A vulnerability has been identified in Spectrum Power 4 (All versions < V4.70 SP8). Insecure storage of sensitive information in the configuration files could allow the retrieval of user names.	5.3	More Details
CVE-2020-25249	An issue was discovered in Hyland OnBase 16.0.2.83 and below, 17.0.2.109 and below, 18.0.0.37 and below, 19.8.16.1000 and below and 20.3.10.1000 and below. The server typically logs activity only when a client application specifies that logging is desired. This can be problematic for use cases in a regulated industry, where server-side logging is required in additional situations.	5.3	More Details
CVE-2020-9743	AEM versions 6.5.5.0 (and below), 6.4.8.1 (and below), 6.3.3.8 (and below) and 6.2 SP1-CFP20 (and below) are affected by an HTML injection vulnerability in the content editor component that allows unauthenticated users to craft an HTTP request that includes arbitrary HTML code in a parameter value. An attacker could then use the malicious GET request to lure victims to perform unsafe actions in the page (ex. phishing).	5.3	More Details
CVE-2020-5780	Missing Authentication for Critical Function in Icegram Email Subscribers & Newsletters Plugin for WordPress prior to version 4.5.6 allows a remote, unauthenticated attacker to conduct unauthenticated email forgery/spoofing.	5.3	More Details
CVE-2020-0805	A security feature bypass vulnerability exists when a Windows Projected Filesystem improperly handles file redirections. An attacker who successfully exploited this vulnerability could delete a targeted file they would not have permissions to. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability. The security update addresses the vulnerability by correcting how Windows Projected Filesystem handle file redirections.	5.3	More Details
CVE-2020-24655	A race condition in the Twilio Authy 2-Factor Authentication application before 24.3.7 for Android allows a user to potentially approve/deny an access request prior to unlocking the application with a PIN on older Android devices (effectively bypassing the PIN requirement).	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0837	An elevation of privilege vulnerability exists when Active Directory Federation Services (ADFS) improperly handles multi-factor authentication requests. An attacker who successfully exploited this vulnerability could bypass some, but not all, of the authentication factors. To exploit this vulnerability, an attacker could send a specially crafted authentication request. This security update corrects how ADFS handles multi-factor authentication requests.	5.0	More Details
CVE-2020-16214	In Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, the software saves user-provided information into a comma-separated value (CSV) file, but it does not neutralize or incorrectly neutralizes special elements that could be interpreted as a command when the file is opened by spreadsheet software.	5.0	More Details
CVE-2020-14330	An Improper Output Neutralization for Logs flaw was found in Ansible when using the uri module, where sensitive data is exposed to content and json output. This flaw allows an attacker to access the logs or outputs of performed tasks to read keys used in playbooks from other users within the uri module. The highest threat from this vulnerability is to data confidentiality.	5.0	More Details
CVE-2020-7068	In PHP versions 7.2.x below 7.2.33, 7.3.x below 7.3.21 and 7.4.x below 7.4.9, while processing PHAR files using phar extension, phar_parse_zipfile could be tricked into accessing freed memory, which could lead to a crash or information disclosure.	4.8	More Details
CVE-2020-7322	Information Disclosure Vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local users to gain access to sensitive information via incorrectly logging of sensitive information in debug logs.	4.7	More Details
CVE-2020-16873	A spoofing vulnerability manifests in Microsoft Xamarin.Forms due to the default settings on Android WebView version prior to 83.0.4103.106. This vulnerability could allow an attacker to execute arbitrary Javascript code on a target system. For the attack to be successful, the targeted user would need to browse to a malicious website or a website serving the malicious code through Xamarin.Forms. The security update addresses this vulnerability by preventing the malicious Javascript from running in the WebView.	4.7	More Details
CVE-2018-17766	Ingenico Telium 2 POS Telium2 OS allow bypass of file-reading restrictions via the NTPT3 protocol. This is fixed in Telium 2 SDK v9.32.03 patch N.	4.6	More Details
CVE-2020-7294	Privilege Escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows authenticated user interface user to delete or download protected files via improper access controls in the REST interface.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1205	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	4.6	More Details
CVE-2019-14759	An issue was discovered in KaiOS 1.0, 2.5, and 2.5.1. The pre-installed Radio application is vulnerable to HTML and JavaScript injection attacks. A local attacker can inject arbitrary HTML into the Radio application. At a bare minimum, this allows an attacker to take control over the Radio application's UI (e.g., display a malicious prompt to the user asking them to re-enter credentials such as their KaiOS credentials to continue using the application) and also allows an attacker to abuse any of the privileges available to the mobile application.	4.4	More Details
CVE-2019-14760	An issue was discovered in KaiOS 2.5. The pre-installed Recorder application is vulnerable to HTML and JavaScript injection attacks. A local attacker can inject arbitrary HTML into the Recorder application. At a bare minimum, this allows an attacker to take control over the Recorder application's UI (e.g., display a malicious prompt to the user asking them to re-enter credentials such as their KaiOS credentials to continue using the application) and also allows an attacker to abuse any of the privileges available to the mobile application.	4.4	More Details
CVE-2020-10773	A stack information leak flaw was found in s390/s390x in the Linux kernel’s memory manager functionality, where it incorrectly writes to the /proc/sys/vm/cmm_timeout file. This flaw allows a local user to see the kernel data.	4.4	More Details
CVE-2019-14761	An issue was discovered in KaiOS 2.5. The pre-installed Note application is vulnerable to HTML and JavaScript injection attacks. A local attacker can inject arbitrary HTML into the Note application. At a bare minimum, this allows an attacker to take control over the Note application's UI (e.g., display a malicious prompt to the user asking them to re-enter credentials such as their KaiOS credentials to continue using the application) and also allows an attacker to abuse any of the privileges available to the mobile application.	4.4	More Details
CVE-2020-1592	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user’s system. The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14304	A memory disclosure flaw was found in the Linux kernel's ethernet drivers, in the way it read data from the EEPROM of the device. This flaw allows a local user to read uninitialized values from the kernel memory. The highest threat from this vulnerability is to confidentiality.	4.4	More Details
CVE-2020-14342	It was found that cifs-utils' mount.cifs was invoking a shell when requesting the Samba password, which could be used to inject arbitrary commands. An attacker able to invoke mount.cifs with special permission, such as via sudo rules, could use this flaw to escalate their privileges.	4.4	More Details
CVE-2020-1589	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user’s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.	4.4	More Details
CVE-2020-6344	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PDF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6350	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated BMP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6340	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6354	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated SKP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6353	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated SKP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6352	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated FBX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6351	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated FBX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6339	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated BMP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6343	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated EPS file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6349	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated GIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-16099	In Gallagher Command Centre v8.20 prior to v8.20.1093(MR2) it is possible to create Guard Tour events that when accessed via things like reporting cause clients to temporarily hang or disconnect.	4.3	More Details
CVE-2020-6348	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated GIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-13311	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Wiki was vulnerable to a parser attack that prohibits anyone from accessing the Wiki functionality through the user interface.	4.3	More Details
CVE-2020-6338	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated RH file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6337	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HDR file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6347	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HDR file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6341	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated EPS file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6336	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6346	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated BMP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6335	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HPGL file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6345	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated TGA file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6355	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated TGA file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-13313	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. An unauthorized project maintainer could edit the subgroup badges due to the lack of authorization control.	4.3	More Details
CVE-2020-6356	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated BMP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6331	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HPGL file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1044	A security feature bypass vulnerability exists in SQL Server Reporting Services (SSRS) when the server improperly validates attachments uploaded to reports. An attacker who successfully exploited this vulnerability could upload file types that were disallowed by an administrator. To exploit the vulnerability, an authenticated attacker would need to send a specially crafted request to an affected SSRS server. The update addresses the vulnerability by modifying how SSRS validates attachment uploads.	4.3	More Details
CVE-2020-6314	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HPGL file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6322	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated 3DM file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2018-19947	The vulnerability have been reported to affect earlier versions of Helpdesk. If exploited, this information exposure vulnerability could disclose sensitive information. QNAP has already fixed the issue in Helpdesk 3.0.3 and later.	4.3	More Details
CVE-2020-6327	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated 3DM file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6328	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated CGM file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6329	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated SKP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6357	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated U3D file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8339	A cross-site scripting inclusion (XSSI) vulnerability was reported in the legacy IBM BladeCenter Advanced Management Module (AMM) web interface prior to version 3.68n [BPET68N]. This vulnerability could allow an authenticated user's AMM credentials to be disclosed if the user is convinced to visit a malicious web site, possibly through phishing. Successful exploitation requires specific knowledge about the user's network to be included in the malicious web site. Impact is limited to the normal access restrictions of the user visiting the malicious web site, and subject to the user being logged into AMM, being able to connect to both AMM and the malicious web site while the web browser is open, and using a web browser that does not inherently protect against this class of attack. The JavaScript code is not executed on AMM itself.	4.3	More Details
CVE-2020-6330	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated 3DM file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6332	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated HPGL file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-16220	In Patient Information Center iX (PICiX) Versions C.02, C.03, PerformanceBridge Focal Point Version A.01, the product receives input that is expected to be well-formed (i.e., to comply with a certain syntax) but it does not validate or incorrectly validates that the input complies with the syntax, causing the certificate enrollment service to crash. It does not impact monitoring but prevents new devices from enrolling.	4.3	More Details
CVE-2020-4526	IBM Maximo Asset Management 7.6.0 and 7.6.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 182436.	4.3	More Details
CVE-2020-6333	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated 3DM file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6342	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated U3D file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6361	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated RLE files received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6360	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated DIB file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6359	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PLT file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-6358	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated FBX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2020-13287	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Project reporters and above could see confidential EPIC attached to confidential issues	4.3	More Details
CVE-2020-6334	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated SKP file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.	4.3	More Details
CVE-2018-19946	The vulnerability have been reported to affect earlier versions of Helpdesk. If exploited, this improper certificate validation vulnerability could allow an attacker to spoof a trusted entity by interfering in the communication path between the host and client. QNAP has already fixed the issue in Helpdesk 3.0.3 and later.	4.2	More Details
CVE-2020-1180	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how the ChakraCore scripting engine handles objects in memory.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1172	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how the ChakraCore scripting engine handles objects in memory.	4.2	More Details
CVE-2020-0878	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory. The vulnerability could corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, the attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers, and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically via an enticement in email or instant message, or by getting them to open an email attachment. The security update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory.	4.2	More Details
CVE-2020-1057	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how the ChakraCore scripting engine handles objects in memory.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16884	A remote code execution vulnerability exists in the way that the IEToEdge Browser Helper Object (BHO) plugin on Internet Explorer handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how the IEToEdge BHO plug-in handles objects in memory.	4.2	More Details
CVE-2020-25284	The rbd block device driver in drivers/block/rbd.c in the Linux kernel through 5.8.9 used incomplete permission checking for access to rbd devices, which could be leveraged by local attackers to map or unmap rbd block devices, aka CID-f44d04e696fe.	4.1	More Details
CVE-2020-1033	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user’s system. An authenticated attacker could exploit this vulnerability by running a specially crafted application. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.	4.0	More Details
CVE-2020-13307	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was not revoking current user sessions when 2 factor authentication was activated allowing a malicious user to maintain their access.	3.8	More Details
CVE-2020-13304	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Same 2 factor Authentication secret code was generated which resulted an attacker to maintain access under certain conditions.	3.8	More Details
CVE-2020-13302	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Under certain conditions GitLab was not properly revoking user sessions and allowed a malicious user to access a user account with an old password.	3.8	More Details
CVE-2014-1420	On desktop, Ubuntu UI Toolkit's StateSaver would serialise data on tmp/ files which an attacker could use to expose potentially sensitive data. StateSaver would also open files without the O_EXCL flag. An attacker could exploit this to launch a symlink attack, though this is partially mitigated by symlink and hardlink restrictions in Ubuntu. Fixed in 1.1.1188+14.10.20140813.4-0ubuntu1.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13297	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. When 2 factor authentication was enabled for groups, a malicious user could bypass that restriction by sending a specific query to the API endpoint.	3.8	More Details
CVE-2020-13314	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab Omniauth endpoint allowed a malicious user to submit content to be displayed back to the user within error messages.	3.7	More Details
CVE-2020-13306	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab Webhook feature could be abused to perform denial of service attacks due to the lack of rate limitation.	3.7	More Details
CVE-2020-1968	The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).	3.7	More Details
CVE-2020-13315	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. The profile activity page was not restricting the amount of results one could request, potentially resulting in a denial of service.	3.7	More Details
CVE-2020-7295	Privilege Escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows authenticated user interface user to delete or download protected log data via improper access controls in the user interface.	3.5	More Details
CVE-2020-16218	In Patient Information Center iX (PICiX) Versions B.02, C.02, C.03, the software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is then used as a webpage and served to other users. Successful exploitation could lead to unauthorized access to patient data via a read-only web application.	3.5	More Details
CVE-2020-13305	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was not invalidating project invitation link upon removing a user from a project.	3.5	More Details
CVE-2020-4344	IBM Tivoli Business Service Manager 6.2.0.0 - 6.2.0.2 IF 1 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 178247.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2043	An information exposure through log file vulnerability where sensitive fields are recorded in the configuration log without masking on Palo Alto Networks PAN-OS software when the after-change-detail custom syslog field is enabled for configuration logs and the sensitive field appears multiple times in one log entry. The first instance of the sensitive field is masked but subsequent instances are left in clear text. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.4.	3.3	More Details
CVE-2020-2044	An information exposure through log file vulnerability where an administrator's password or other sensitive information may be logged in cleartext while using the CLI in Palo Alto Networks PAN-OS software. The opcmdhistory.log file was introduced to track operational command (op-command) usage but did not mask all sensitive information. The opcmdhistory.log file is removed in PAN-OS 9.1 and later PAN-OS versions. Command usage is recorded, instead, in the req_stats.log file in PAN-OS 9.1 and later PAN-OS versions. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.10; PAN-OS 9.1 versions earlier than PAN-OS 9.1.3.	3.3	More Details
CVE-2020-13308	A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. A user without 2 factor authentication enabled could be prohibited from accessing GitLab by being invited into a project that had 2 factor authentication inheritance.	2.7	More Details
CVE-2020-15168	node-fetch before versions 2.6.1 and 3.0.0-beta.9 did not honor the size option after following a redirect, which means that when a content size was over the limit, a FetchError would never get thrown and the process would end without failure. For most people, this fix will have a little or no impact. However, if you are relying on node-fetch to gate files above a size, the impact could be significant, for example: If you don't double-check the size of the data after fetch() has completed, your JS thread could get tied up doing work on a large file (DoS) and/or cost you money in computing.	2.6	More Details
CVE-2018-19948	The vulnerability have been reported to affect earlier versions of Helpdesk. If exploited, this cross-site request forgery (CSRF) vulnerability could allow attackers to force NAS users to execute unintentional actions through a web application. QNAP has already fixed the issue in Helpdesk 3.0.3 and later.	2.0	More Details
CVE-2019-1554	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-2019-1539	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-2019-1540	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 Number	Description	Base Score	Reference
CVE-2019-1541	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-2019-1550	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-2019-1553	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-2019-1542	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-2019-1544	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-2019-1545	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-2019-1538	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-2019-1546	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-2019-1558	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-2019-1537	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-2019-1555	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-2019-1536	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 Number	Description	Base Score	Reference
CVE-2019-1556	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-2019-1535	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-2019-1557	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-2019-1560	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-2019-1561	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-2019-1562	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-2019-1564	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-2020-24200	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-2019-1548	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