SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 March 2021

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-21322	fastify-http-proxy is an npm package which is a fastify plugin for proxying your http requests to another server, with hooks. By crafting a specific URL, it is possible to escape the prefix of the proxied backend service. If the base url of the proxied server is `/pub/`, a user expect that accessing `/priv` on the target service would not be possible. In affected versions, it is possible. This is fixed in version 4.3.1.	10.0	More Details
CVE-2021-21321	fastify-reply-from is an npm package which is a fastify plugin to forward the current http request to another server. In fastify-reply-from before version 4.0.2, by crafting a specific URL, it is possible to escape the prefix of the proxied backend service. If the base url of the proxied server is "/pub/", a user expect that accessing "/priv" on the target service would not be possible. In affected versions, it is possible. This is fixed in version 4.0.2.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1388	A vulnerability in an API endpoint of Cisco ACI Multi-Site Orchestrator (MSO) installed on the Application Services Engine could allow an unauthenticated, remote attacker to bypass authentication on an affected device. The vulnerability is due to improper token validation on a specific API endpoint. An attacker could exploit this vulnerability by sending a crafted request to the affected API. A successful exploit could allow the attacker to receive a token with administrator-level privileges that could be used to authenticate to the API on affected MSO and managed Cisco Application Policy Infrastructure Controller (APIC) devices.	10.0	More Details
CVE-2019-11684	Improper Access Control in the RCP+ server of the Bosch Video Recording Manager (VRM) component allows arbitrary and unauthenticated access to a limited subset of certificates, stored in the underlying Microsoft Windows operating system. The fixed versions implement modified authentication checks. Prior releases of VRM software version 3.70 are considered unaffected. This vulnerability affects VRM v3.70.x, v3.71 < v3.71.0034 and v3.81 < 3.81.0050; DIVAR IP 5000 3.80 < 3.80.0039; BVMS all versions using VRM.	9.9	More Details
CVE-2021-20658	SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an attacker to execute arbitrary OS commands with the web server privilege via unspecified vectors.	9.8	More Details
CVE-2021-25833	A file extension handling issue was found in [server] module of ONLYOFFICE DocumentServer v4.2.0.71-v5.6.0.21. The file extension is controlled by an attacker through the request data and leads to arbitrary file overwriting. Using this vulnerability, a remote attacker can obtain remote code execution on DocumentServer.	9.8	More Details
CVE-2021-3148	An issue was discovered in SaltStack Salt before 3002.5. Sending crafted web requests to the Salt API can result in salt.utils.thin.gen_thin() command injection because of different handling of single versus double quotes. This is related to salt/utils/thin.py.	9.8	More Details
CVE-2021-3197	An issue was discovered in SaltStack Salt before 3002.5. The salt-api's ssh client is vulnerable to a shell injection by including ProxyCommand in an argument, or via ssh_options provided in an API request.	9.8	More Details
CVE-2021-27132	SerComm AG Combo VD625 AGSOT_2.1.0 devices allow CRLF injection (for HTTP header injection) in the download function via the Content-Disposition header.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25830	A file extension handling issue was found in [core] module of ONLYOFFICE DocumentServer v4.2.0.236-v5.6.4.13. An attacker must request the conversion of the crafted file from DOCT into DOCX format. Using the chain of two other bugs related to improper string handling, an attacker can achieve remote code execution on DocumentServer.	9.8	More Details
CVE-2021-25831	A file extension handling issue was found in [core] module of ONLYOFFICE DocumentServer v4.0.0-9-v5.6.3. An attacker must request the conversion of the crafted file from PPTT into PPTX format. Using the chain of two other bugs related to improper string handling, a remote attacker can obtain remote code execution on DocumentServer.	9.8	More Details
CVE-2021-25832	A heap buffer overflow vulnerability inside of BMP image processing was found at [core] module of ONLYOFFICE DocumentServer v4.0.0-9-v6.0.0. Using this vulnerability, an attacker is able to gain remote code executions on DocumentServer.	9.8	More Details
CVE-2021-26476	EPrints 3.4.2 allows remote attackers to execute OS commands via crafted LaTeX input to a cgi/cal?year= URI.	9.8	More Details
CVE-2021-25914	Prototype pollution vulnerability in 'object-collider' versions 1.0.0 through 1.0.3 allows attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2019-25022	An issue was discovered in Scytl sVote 2.1. An attacker can inject code that gets executed by creating an election-event and injecting a payload over an event alias, because the application calls Runtime.getRuntime().exec() without validation.	9.8	More Details
CVE-2021-26703	EPrints 3.4.2 allows remote attackers to read arbitrary files and possibly execute commands via crafted JSON/XML input to a cgi/ajax/phrase URI.	9.8	More Details
CVE-2021-3342	EPrints 3.4.2 allows remote attackers to read arbitrary files and possibly execute commands via crafted LaTeX input to a cgi/latex2png?latex= URI.	9.8	More Details
CVE-2021-27886	rakibtg Docker Dashboard before 2021-02-28 allows command injection in backend/utilities/terminal.js via shell metacharacters in the command parameter of an API request. NOTE: this is NOT a Docker, Inc. product.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25309	The telnet administrator service running on port 650 on Gigaset DX600A v41.00-175 devices does not implement any lockout or throttling functionality. This situation (together with the weak password policy that forces a 4-digit password) allows remote attackers to easily obtain administrative access via brute-force attacks.	9.8	More Details
CVE-2021-27804	JPEG XL (aka jpeg-xl) through 0.3.2 allows writable memory corruption.	9.8	More Details
CVE-2021-27730	Accellion FTA 9_12_432 and earlier is affected by argument injection via a crafted POST request to an admin endpoint. The fixed version is FTA_9_12_444 and later.	9.8	More Details
CVE-2021-25283	An issue was discovered in through SaltStack Salt before 3002.5. The jinja renderer does not protect against server side template injection attacks.	9.8	More Details
CVE-2021-25281	An issue was discovered in through SaltStack Salt before 3002.5. salt-api does not honor eauth credentials for the wheel_async client. Thus, an attacker can remotely run any wheel modules on the master.	9.8	More Details
CVE-2021-24077	Windows Fax Service Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-24074	Windows TCP/IP Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-21972	The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. This affects VMware vCenter Server (7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2 and 3.x before 3.10.1.2).	9.8	More Details
CVE-2021-22667	BB-ESWGP506-2SFP-T versions 1.01.09 and prior is vulnerable due to the use of hard-coded credentials, which may allow an attacker to gain unauthorized access and permit the execution of arbitrary code on the BB-ESWGP506-2SFP-T (versions 1.01.01 and prior).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1361	A vulnerability in the implementation of an internal file management service for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode that are running Cisco NX-OS Software could allow an unauthenticated, remote attacker to create, delete, or overwrite arbitrary files with root privileges on the device. This vulnerability exists because TCP port 9075 is incorrectly configured to listen and respond to external connection requests. An attacker could exploit this vulnerability by sending crafted TCP packets to an IP address that is configured on a local interface on TCP port 9075. A successful exploit could allow the attacker to create, delete, or overwrite arbitrary files, including sensitive files that are related to the device configuration. For example, the attacker could add a user account without the device administrator knowing.	9.8	More Details
CVE-2021-1393	Multiple vulnerabilities in Cisco Application Services Engine could allow an unauthenticated, remote attacker to gain privileged access to host-level operations or to learn device-specific information, create diagnostic files, and make limited configuration changes. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2021-1396	Multiple vulnerabilities in Cisco Application Services Engine could allow an unauthenticated, remote attacker to gain privileged access to host-level operations or to learn device-specific information, create diagnostic files, and make limited configuration changes. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2021-27670	Appspace 6.2.4 allows SSRF via the api/v1/core/proxy/jsonprequest url parameter.	9.8	More Details
CVE-2020-23534	A server-side request forgery (SSRF) vulnerability in Upgrade.php of gopeak masterlab 2.1.5, via the 'source' parameter.	9.8	More Details
CVE-2021-3406	A flaw was found in keylime 5.8.1 and older. The issue in the Keylime agent and registrar code invalidates the cryptographic chain of trust from the Endorsement Key certificate to agent attestations.	9.8	More Details
CVE-2020-28657	In bPanel 2.0, the administrative ajax endpoints (aka ajax/aj_*.php) are accessible without authentication and allow SQL injections, which could lead to platform compromise.	9.8	More Details
CVE-2021-24078	Windows DNS Server Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24094	Windows TCP/IP Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-26904	LMA ISIDA Retriever 5.2 allows SQL Injection.	9.8	More Details
CVE-2021-27198	An issue was discovered in Visualware MyConnection Server before v11.1a. Unauthenticated Remote Code Execution can occur via Arbitrary File Upload in the web service when using a myspeed/sf?filename= URI. This application is written in Java and is thus cross-platform. The Windows installation runs as SYSTEM, which means that exploitation gives one Administrator privileges on the target system.	9.8	More Details
CVE-2020-27224	In Eclipse Theia versions up to and including 1.2.0, the Markdown Preview (@theia/preview), can be exploited to execute arbitrary code.	9.6	More Details
CVE-2021-25282	An issue was discovered in through SaltStack Salt before 3002.5. The salt.wheel.pillar_roots.write method is vulnerable to directory traversal.	9.1	More Details
CVE-2020-28199	best it Amazon Pay Plugin before 9.4.2 for Shopware exposes Sensitive Information to an Unauthorized Actor.	9.1	More Details
CVE-2021-3144	In SaltStack Salt before 3002.5, eauth tokens can be used once after expiration. (They might be used to run command against the salt master or minions.)	9.1	More Details
CVE-2021-21515	Dell EMC SourceOne, versions 7.2SP10 and prior, contain a Stored Cross-Site Scripting vulnerability. A remote low privileged attacker may potentially exploit this vulnerability, to hijack user sessions or to trick a victim application user to unknowingly send arbitrary requests to the server.	9.0	More Details
CVE-2021-26560	Cleartext transmission of sensitive information vulnerability in synoagentregisterd in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows man-in-the-middle attackers to spoof servers via an HTTP session.	9.0	More Details
CVE-2021-26561	Stack-based buffer overflow vulnerability in synoagentregisterd in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows man-in-the-middle attackers to execute arbitrary code via syno_finder_site HTTP header.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26562	Out-of-bounds write vulnerability in synoagentregisterd in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows man-in-the-middle attackers to execute arbitrary code via syno_finder_site HTTP header.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-27885	usersettings.php in e107 through 2.3.0 lacks a certain e_TOKEN protection mechanism.	8.8	More Details
CVE-2021-23972	One phishing tactic on the web is to provide a link with HTTP Auth. For example 'https://www.phishingtarget.com@evil.com'. To mitigate this type of attack, Firefox will display a warning dialog; however, this warning dialog would not have been displayed if evil.com used a redirect that was cached by the browser. This vulnerability affects Firefox < 86.	8.8	More Details
CVE-2021-21974	OpenSLP as used in ESXi (7.0 before ESXi70U1c-17325551, 6.7 before ESXi670-202102401-SG, 6.5 before ESXi650-202102101-SG) has a heap-overflow vulnerability. A malicious actor residing within the same network segment as ESXi who has access to port 427 may be able to trigger the heap-overflow issue in OpenSLP service resulting in remote code execution.	8.8	More Details
CVE-2021-1728	System Center Operations Manager Elevation of Privilege Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1368	A vulnerability in the Unidirectional Link Detection (UDLD) feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code with administrative privileges or cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted Cisco UDLD protocol packets to a directly connected, affected device. A successful exploit could allow the attacker to execute arbitrary code with administrative privileges or cause the Cisco UDLD process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition. Note: The UDLD feature is disabled by default, and the conditions to exploit this vulnerability are strict. The attacker needs full control of a directly connected device. That device must be connected over a port channel that has UDLD enabled. To trigger arbitrary code execution, both the UDLD-enabled port channel and specific system conditions must exist. In the absence of either the UDLD-enabled port channel or the system conditions, attempts to exploit this vulnerability will result in a DoS condition. It is possible, but highly unlikely, that an attacker could control the necessary conditions for exploitation. The CVSS score reflects this possibility. However, given the complexity of exploitation, Cisco has assigned a Medium Security Impact Rating (SIR) to this vulnerability.	8.8	More Details
CVE-2021-24066	Microsoft SharePoint Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-23964	Mozilla developers reported memory safety bugs present in Firefox 84 and Firefox ESR 78.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.	8.8	More Details
CVE-2021-23965	Mozilla developers reported memory safety bugs present in Firefox 84. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 85.	8.8	More Details
CVE-2021-23978	Mozilla developers reported memory safety bugs present in Firefox 85 and Firefox ESR 78.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26704	EPrints 3.4.2 allows remote attackers to execute arbitrary commands via crafted input to the verb parameter in a cgi/toolbox/toolbox URI.	8.8	More Details
CVE-2021-21617	A cross-site request forgery (CSRF) vulnerability in Jenkins Configuration Slicing Plugin 1.51 and earlier allows attackers to apply different slice configurations.	8.8	More Details
CVE-2021-24072	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-23954	Using the new logical assignment operators in a JavaScript switch statement could have caused a type confusion, leading to a memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.	8.8	More Details
CVE-2021-23960	Performing garbage collection on re-declared JavaScript variables resulted in a user-after-poison, and a potentially exploitable crash. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.	8.8	More Details
CVE-2021-23979	Mozilla developers reported memory safety bugs present in Firefox 85. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 86.	8.8	More Details
CVE-2021-27878	An issue was discovered in Veritas Backup Exec before 21.2. The communication between a client and an Agent requires successful authentication, which is typically completed over a secure TLS communication. However, due to a vulnerability in the SHA Authentication scheme, an attacker is able to gain unauthorized access and complete the authentication process. Subsequently, the client can execute data management protocol commands on the authenticated connection. The attacker could use one of these commands to execute an arbitrary command on the system using system privileges.	8.8	More Details
CVE-2021-23962	Incorrect use of the '<RowCountChanged>' method could have led to a user-after-poison and a potentially exploitable crash. This vulnerability affects Firefox < 85.	8.8	More Details
CVE-2021-24088	Windows Local Spooler Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24093	Windows Graphics Component Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-20659	SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an authenticated attacker to upload arbitrary files via unspecified vectors. If the file is PHP script, an attacker may execute arbitrary code.	8.8	More Details
CVE-2020-17162	Microsoft Windows Security Feature Bypass Vulnerability	8.8	More Details
CVE-2021-1387	A vulnerability in the network stack of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because the software improperly releases resources when it processes certain IPv6 packets that are destined to an affected device. An attacker could exploit this vulnerability by sending multiple crafted IPv6 packets to an affected device. A successful exploit could cause the network stack to run out of available buffers, impairing operations of control plane and management plane protocols and resulting in a DoS condition. Manual intervention would be required to restore normal operations on the affected device. For more information about the impact of this vulnerability, see the Details section of this advisory.	8.6	More Details
CVE-2021-21513	Dell EMC OpenManage Server Administrator (OMSA) version 9.5 Microsoft Windows installations with Distributed Web Server (DWS) enabled configuration contains an authentication bypass vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to gain admin access on the affected system.	8.6	More Details
CVE-2021-1230	A vulnerability with the Border Gateway Protocol (BGP) for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an unauthenticated, remote attacker to cause a routing process to crash, which could lead to a denial of service (DoS) condition. This vulnerability is due to an issue with the installation of routes upon receipt of a BGP update. An attacker could exploit this vulnerability by sending a crafted BGP update to an affected device. A successful exploit could allow the attacker to cause the routing process to crash, which could cause the device to reload. This vulnerability applies to both Internal BGP (IBGP) and External BGP (EBGP). Note: The Cisco implementation of BGP accepts incoming BGP traffic from explicitly configured peers only. To exploit this vulnerability, an attacker would need to send a specific BGP update message over an established TCP connection that appears to come from a trusted BGP peer.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24105	Depending on configuration of various package managers it is possible for an attacker to insert a malicious package into a package manager's repository which can be retrieved and used during development, build, and release processes. This insertion could lead to remote code execution. We believe this vulnerability affects multiple package managers across multiple languages, including but not limited to: Python/pip, .NET/NuGet, Java/Maven, JavaScript/npm. Attack scenarios An attacker could take advantage of this ecosystem-wide issue to cause harm in a variety of ways. The original attack scenarios were discovered by Alex Birsan and are detailed in their whitepaper, Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies. - With basic knowledge of the target ecosystems, an attacker could create an empty shell for a package and insert malicious code in the install scripts, give it a high version, and publish it to the public repository. Vulnerable victim machines will download the higher version of the package between the public and private repositories and attempt to install it. Due to code incompatibility it will probably error out upon import or upon compilation, making it easier to detect; however the attacker would have gained code execution by that point. - An advanced attacker with some inside knowledge of the target could take a copy of a working package, insert the malicious code (in the package itself or in the install), and then publish it to a public repository. The package will likely install and import correctly, granting the attacker an initial foothold and persistence. These two methods could affect target organizations at any of these various levels: - Developer machines - An entire team if the configuration to import the malicious package is uploaded to a code repository - Continuous integration pipelines if they pull the malicious packages during the build, test, and/or deploy stages - Customers, download servers, production services if the malicious code has not been detected This remote code execution vulnerability can only be addressed by reconfiguring installation tools and workflows, and not by correcting anything in the package repositories themselves. See the FAQ section of this CVE for configuration guidance.	8.4	More Details
CVE-2021-26566	Insertion of sensitive information into sent data vulnerability in synorelayd in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows man-in-the-middle attackers to execute arbitrary commands via inbound QuickConnect traffic.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26565	Cleartext transmission of sensitive information vulnerability in synorelayd in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows man-in-the-middle attackers to obtain sensitive information via an HTTP session.	8.3	More Details
CVE-2021-26564	Cleartext transmission of sensitive information vulnerability in synorelayd in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows man-in-the-middle attackers to spoof servers via an HTTP session.	8.3	More Details
CVE-2021-26563	Incorrect authorization vulnerability in synoagentregisterd in Synology DiskStation Manager (DSM) before 6.2.4-25553 allows local users to execute arbitrary code via unspecified vectors.	8.2	More Details
CVE-2020-11988	Apache XmlGraphics Commons 2.4 and earlier is vulnerable to server-side request forgery, caused by improper input validation by the XMPParser. By using a specially-crafted argument, an attacker could exploit this vulnerability to cause the underlying server to make arbitrary GET requests. Users should upgrade to 2.6 or later.	8.2	More Details
CVE-2020-11987	Apache Batik 1.13 is vulnerable to server-side request forgery, caused by improper input validation by the NodePickerPanel. By using a specially-crafted argument, an attacker could exploit this vulnerability to cause the underlying server to make arbitrary GET requests.	8.2	More Details
CVE-2021-27877	An issue was discovered in Veritas Backup Exec before 21.2. It supports multiple authentication schemes: SHA authentication is one of these. This authentication scheme is no longer used in current versions of the product, but hadn't yet been disabled. An attacker could remotely exploit this scheme to gain unauthorized access to an Agent and execute privileged commands.	8.2	More Details
CVE-2021-1722	Windows Fax Service Remote Code Execution Vulnerability	8.1	More Details
CVE-2020-36254	scp.c in Dropbear before 2020.79 mishandles the filename of . or an empty filename, a related issue to CVE-2018-20685.	8.1	More Details
CVE-2021-26701	.NET Core Remote Code Execution Vulnerability	8.1	More Details
CVE-2021-24112	.NET Core Remote Code Execution Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23976	When accepting a malicious intent from other installed apps, Firefox for Android accepted manifests from arbitrary file paths and allowed declaring webapp manifests for other origins. This could be used to gain fullscreen access for UI spoofing and could also lead to cross-origin attacks on targeted websites. Note: This issue is a different issue from CVE-2020-26954 and only affected Firefox for Android. Other operating systems are unaffected. This vulnerability affects Firefox < 86.	8.1	More Details
CVE-2021-27876	An issue was discovered in Veritas Backup Exec before 21.2. The communication between a client and an Agent requires successful authentication, which is typically completed over a secure TLS communication. However, due to a vulnerability in the SHA Authentication scheme, an attacker is able to gain unauthorized access and complete the authentication process. Subsequently, the client can execute data management protocol commands on the authenticated connection. By using crafted input parameters in one of these commands, an attacker can access an arbitrary file on the system using System privileges.	8.1	More Details
CVE-2021-20661	Directory traversal vulnerability in SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows authenticated attackers to delete arbitrary files and/or directories on the server via unspecified vectors.	8.1	More Details
CVE-2021-1227	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the NX-API on an affected device. An attacker could exploit this vulnerability by persuading a user of the NX-API to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. The attacker could view and modify the device configuration. Note: The NX-API feature is disabled by default.	8.1	More Details
CVE-2021-1726	Microsoft SharePoint Server Spoofing Vulnerability	8.0	More Details
CVE-2020-7846	Helpcom before v10.0 contains a file download and execution vulnerability caused by storing hardcoded cryptographic key. It finally leads to a file download and execution via access to crafted web page.	8.0	More Details
CVE-2021-1733	Sysinternals PsExec Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1727	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-7836	VOICEYE WSActiveBridgeES versions prior to 2.1.0.3 contains a stack-based buffer overflow vulnerability caused by improper bound checking parameter given by attack. It finally leads to a stack-based buffer overflow via access to crafted web page.	7.8	More Details
CVE-2020-28243	An issue was discovered in SaltStack Salt before 3002.5. The minion's restartcheck is vulnerable to command injection via a crafted process name. This allows for a local privilege escalation by any user able to create a files on the minion in a non-blacklisted directory.	7.8	More Details
CVE-2021-1732	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-24068	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-24081	Microsoft Windows Codecs Library Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-24067	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-24069	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-24070	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-26700	Visual Studio Code npm-script Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-28599	A stack-based buffer overflow vulnerability exists in the import_stl.cc:import_stl() functionality of Openscad openscad-2020.12-RC2. A specially crafted STL file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24083	Windows Address Book Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-24096	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-24092	Microsoft Defender Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-24103	Windows Event Tracing Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-24102	Windows Event Tracing Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-21066	Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-26567	Stack-based buffer overflow vulnerability in frontend/main.c in faad2 before 2.2.7.1 allow local attackers to execute arbitrary code via filename and pathname options.	7.8	More Details
CVE-2021-25195	Windows PKU2U Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-24091	Windows Camera Codec Pack Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-28646	ownCloud owncloud/client before 2.7 allows DLL Injection. The desktop client loaded development plugins from certain directories when they were present.	7.8	More Details
CVE-2021-1698	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21297	Node-Red is a low-code programming for event-driven applications built using nodejs. Node-RED 1.2.7 and earlier contains a Prototype Pollution vulnerability in the admin API. A badly formed request can modify the prototype of the default JavaScript Object with the potential to affect the default behaviour of the Node-RED runtime. The vulnerability is patched in the 1.2.8 release. A workaround is to ensure only authorized users are able to access the editor url.	7.7	More Details
CVE-2021-20662	Missing authentication for critical function in SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an attacker to alter the setting information without the access privileges via unspecified vectors.	7.5	More Details
CVE-2021-27799	ean_leading_zeroes in backend/upcean.c in Zint Barcode Generator 2.9.1 has a stack-based buffer overflow that is reachable from the C API through an application that includes the Zint Barcode Generator library code.	7.5	More Details
CVE-2019-25020	An issue was discovered in Scytl sVote 2.1. Because the sdm-ws-rest API does not require authentication, an attacker can retrieve the administrative configuration by sending a POST request to the /sdm-ws-rest/preconfiguration URI.	7.5	More Details
CVE-2021-24111	.NET Framework Denial of Service Vulnerability	7.5	More Details
CVE-2021-24086	Windows TCP/IP Denial of Service Vulnerability	7.5	More Details
CVE-2021-27803	A vulnerability was discovered in how p2p/p2p_pd.c in wpa_supplicant before 2.10 processes P2P (Wi-Fi Direct) provision discovery requests. It could result in denial of service or other impact (potentially execution of arbitrary code), for an attacker within radio range.	7.5	More Details
CVE-2021-25306	A buffer overflow vulnerability in the AT command interface of Gigaset DX600A v41.00-175 devices allows remote attackers to force a device reboot by sending relatively long AT commands.	7.5	More Details
CVE-2019-25021	An issue was discovered in Scytl sVote 2.1. Due to the implementation of the database manager, an attacker can access the OrientDB by providing admin as the admin password. A different password cannot be set because of the implementation in code.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25330	Calling of non-existent provider in MobileWips application prior to SMR Feb-2021 Release 1 allows unauthorized actions including denial of service attack by hijacking the provider.	7.5	More Details
CVE-2021-1734	Windows Remote Procedure Call Information Disclosure Vulnerability	7.5	More Details
CVE-2021-22661	Changing the password on the module webpage does not require the user to type in the current password first. Thus, the password could be changed by a user or external process without knowledge of the current password on the ICX35-HWC-A and ICX35-HWC-E (Versions 1.9.62 and prior).	7.5	More Details
CVE-2021-25122	When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41 and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request.	7.5	More Details
CVE-2021-25829	An improper binary stream data handling issue was found in the [core] module of ONLYOFFICE DocumentServer v4.0.0-9-v5.6.3. Using this bug, an attacker is able to produce a denial of service attack that can eventually shut down the target server.	7.5	More Details
CVE-2020-27543	The restify-paginate package 0.0.5 for Node.js allows remote attackers to cause a Denial-of-Service by omitting the HTTP Host header. A Restify-based web service would crash with an uncaught exception.	7.5	More Details
CVE-2020-24686	The vulnerabilities can be exploited to cause the web visualization component of the PLC to stop and not respond, leading to genuine users losing remote visibility of the PLC state. If a user attempts to login to the PLC while this vulnerability is exploited, the PLC will show an error state and refuse connections to Automation Builder. The execution of the PLC application is not affected by this vulnerability. This issue affects ABB AC500 V2 products with onboard Ethernet.	7.5	More Details
CVE-2020-35662	In SaltStack Salt before 3002.5, when authenticating to services using certain modules, the SSL certificate is not always validated.	7.4	More Details
CVE-2021-23957	Navigations through the Android-specific `intent` URL scheme could have been misused to escape iframe sandbox. Note: This issue only affected Firefox for Android. Other operating systems are unaffected. This vulnerability affects Firefox < 85.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23961	Further techniques that built on the slipstream research combined with a malicious webpage could have exposed both an internal network's hosts as well as services running on the user's local machine. This vulnerability affects Firefox < 85.	7.4	More Details
CVE-2021-1228	A vulnerability in the fabric infrastructure VLAN connection establishment of Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to bypass security validations and connect an unauthorized server to the infrastructure VLAN. This vulnerability is due to insufficient security requirements during the Link Layer Discovery Protocol (LLDP) setup phase of the infrastructure VLAN. An attacker could exploit this vulnerability by sending a crafted LLDP packet on the adjacent subnet to an affected device. A successful exploit could allow the attacker to connect an unauthorized server to the infrastructure VLAN, which is highly privileged. With a connection to the infrastructure VLAN, the attacker can make unauthorized connections to Cisco Application Policy Infrastructure Controller (APIC) services or join other host endpoints.	7.4	More Details
CVE-2019-18945	Micro Focus Solutions Business Manager Application Repository versions prior to 11.7.1 are vulnerable to privilege escalation vulnerability.	7.3	More Details
CVE-2021-21517	SRS Policy Manager 6.X is affected by an XML External Entity Injection (XXE) vulnerability due to a misconfigured XML parser that processes user-supplied DTD input without sufficient validation. A remote unauthenticated attacker can potentially exploit this vulnerability to read system files as a non-root user and may be able to temporarily disrupt the ESRS service.	7.2	More Details
CVE-2020-36079	Zenphoto through 1.5.7 is affected by authenticated arbitrary file upload, leading to remote code execution. The attacker must navigate to the uploader plugin, check the elFinder box, and then drag and drop files into the Files(elFinder) portion of the UI. This can, for example, place a .php file in the server's uploaded/ directory. NOTE: the vendor disputes this because exploitation can only be performed by an admin who has "lots of other possibilities to harm a site.	7.2	More Details
CVE-2021-3273	Nagios XI below 5.7 is affected by code injection in the /nagiosxi/admin/graphtemplates.php component. To exploit this vulnerability, someone must have an admin user account in Nagios XI's web system.	7.2	More Details
CVE-2021-24087	Azure IoT CLI extension Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1639	Visual Studio Code Remote Code Execution Vulnerability	7.0	More Details
CVE-2021-25329	The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue.	7.0	More Details
CVE-2020-26200	A component of Kaspersky custom boot loader allowed loading of untrusted UEFI modules due to insufficient check of their authenticity. This component is incorporated in Kaspersky Rescue Disk (KRD) and was trusted by the Authentication Agent of Full Disk Encryption in Kaspersky Endpoint Security (KES). This issue allowed to bypass the UEFI Secure Boot security feature. An attacker would need physical access to the computer to exploit it. Otherwise, local administrator privileges would be required to modify the boot loader component.	6.8	More Details
CVE-2021-24109	Microsoft Azure Kubernetes Service Elevation of Privilege Vulnerability	6.8	More Details
CVE-2021-21302	PrestaShop is a fully scalable open source e-commerce solution. In PrestaShop before version 1.7.2 there is a CSV Injection vulnerability possible by using shop search keywords via the admin panel. The problem is fixed in 1.7.7.2	6.8	More Details
CVE-2021-27901	An issue was discovered on LG mobile devices with Android OS 11 software. They mishandle fingerprint recognition because local high beam mode (LHBM) does not function properly during bright illumination. The LG ID is LVE-SMP-210001 (March 2021).	6.8	More Details
CVE-2021-24075	Microsoft Windows VMSwitch Denial of Service Vulnerability	6.8	More Details
CVE-2021-21258	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI from version 9.5.0 and before version 9.5.4, there is a cross-site scripting injection vulnerability when using ajax/kanban.php. This is fixed in version 9.5.4.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0402	In jpeg, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05433311.	6.7	More Details
CVE-2020-8032	A Insecure Temporary File vulnerability in the packaging of cyrus-sasl of openSUSE Factory allows local attackers to escalate to root. This issue affects: openSUSE Factory cyrus-sasl version 2.1.27-4.2 and prior versions.	6.7	More Details
CVE-2021-0406	In cameraisp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-10, Android-11; Patch ID: ALPS05471418.	6.7	More Details
CVE-2021-0405	In performance driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-10, Android-11; Patch ID: ALPS05466547.	6.7	More Details
CVE-2020-24455	Missing initialization of a variable in the TPM2 source may allow a privileged user to potentially enable an escalation of privilege via local access. This affects tpm2-tss before 3.0.1 and before 2.4.3.	6.7	More Details
CVE-2021-24101	Microsoft Dataverse Information Disclosure Vulnerability	6.5	More Details
CVE-2021-23975	The developer page about:memory has a Measure function for exploring what object types the browser has allocated and their sizes. When this function was invoked we incorrectly called the sizeof function, instead of using the API method that checks for invalid pointers. This vulnerability affects Firefox < 86.	6.5	More Details
CVE-2020-12528	An issue was discovered in MB connect line mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. Improper use of access validation allows a logged in user to kill web2go sessions in the account he should not have access to.	6.5	More Details
CVE-2020-4931	IBM MQ 9.1 LTS, 9.2 LTS, and 9.1 CD AMQP Channels could allow an authenticated user to cause a denial of service due to an issue processing messages. IBM X-Force ID: 191747.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12527	An issue was discovered in MB connect line mymbCONNECT24, mbCONNECT24 and Helmholz myREX24 and myREX24.virtual in all versions through v2.11.2. Improper access validation allows a logged in user to shutdown or reboot devices in his account without having corresponding permissions.	6.5	More Details
CVE-2021-23958	The browser could have been confused into transferring a screen sharing state into another tab, which would leak unintended information. This vulnerability affects Firefox < 85.	6.5	More Details
CVE-2021-24099	Skype for Business and Lync Denial of Service Vulnerability	6.5	More Details
CVE-2021-23956	An ambiguous file picker design could have confused users who intended to select and upload a single file into uploading a whole directory. This was addressed by adding a new prompt. This vulnerability affects Firefox < 85.	6.5	More Details
CVE-2020-7929	A user authorized to perform database queries may trigger denial of service by issuing specially crafted query contain a type of regex. This issue affects MongoDB Server v3.6 versions prior to 3.6.21 and MongoDB Server v4.0 versions prior to 4.0.20.	6.5	More Details
CVE-2021-24073	Skype for Business and Lync Spoofing Vulnerability	6.5	More Details
CVE-2021-24080	Windows Trust Verification API Denial of Service Vulnerability	6.5	More Details
CVE-2021-23973	When trying to load a cross-origin resource in an audio/video context a decoding error may have resulted, and the content of that error may have revealed information about the resource. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.	6.5	More Details
CVE-2021-1721	.NET Core and Visual Studio Denial of Service Vulnerability	6.5	More Details
CVE-2019-25023	An issue was discovered in Scytl sVote 2.1. Because the IP address from an X-Forwarded-For header (which can be manipulated client-side) is used for the internal application logs, an attacker can inject wrong IP addresses into these logs.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24085	Microsoft Exchange Server Spoofing Vulnerability	6.5	More Details
CVE-2021-23971	When processing a redirect with a conflicting Referrer-Policy, Firefox would have adopted the redirect's Referrer-Policy. This would have potentially resulted in more information than intended by the original origin being provided to the destination of the redirect. This vulnerability affects Firefox < 86.	6.5	More Details
CVE-2021-23970	Context-specific code was included in a shared jump table; resulting in assertions being triggered in multithreaded wasm code. This vulnerability affects Firefox < 86.	6.5	More Details
CVE-2021-0367	In vpu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-10, Android-11; Patch ID: ALPS05371580; Issue ID: ALPS05379085.	6.4	More Details
CVE-2021-20328	Specific versions of the Java driver that support client-side field level encryption (CSFLE) fail to perform correct host name verification on the KMS server’s certificate. This vulnerability in combination with a privileged network position active MITM attack could result in interception of traffic between the Java driver and the KMS service rendering Field Level Encryption ineffective. This issue was discovered during internal testing and affects all versions of the Java driver that support CSFLE. The Java async, Scala, and reactive streams drivers are not impacted. This vulnerability does not impact driver traffic payloads with CSFLE-supported key services originating from applications residing inside the AWS, GCP, and Azure network fabrics due to compensating controls in these environments. This issue does not impact driver workloads that don’t use Field Level Encryption.	6.4	More Details
CVE-2021-0401	In vow, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-10, Android-11; Patch ID: ALPS05418265.	6.4	More Details
CVE-2021-0366	In vpu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-10, Android-11; Patch ID: ALPS05371580; Issue ID: ALPS05379093.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20327	A specific version of the Node.js mongodb-client-encryption module does not perform correct validation of the KMS server's certificate. This vulnerability in combination with a privileged network position active MITM attack could result in interception of traffic between the Node.js driver and the KMS service rendering client-side field level encryption (CSFLE) ineffective. This issue was discovered during internal testing and affects mongodb-client-encryption module version 1.2.0, which was available from 2021-Jan-29 and deprecated in the NPM Registry on 2021-Feb-04. This vulnerability does not impact driver traffic payloads with CSFLE-supported key services from applications residing inside the AWS, GCP, and Azure nework fabrics due to compensating controls in these environments. This issue does not impact driver workloads that don't use Field Level Encryption. This issue affect MongoDB Node.js Driver mongodb-client-encryption module version 1.2.0	6.4	More Details
CVE-2021-27318	Cross Site Scripting (XSS) vulnerability in contactus.php in Doctor Appointment System 1.0 allows remote attackers to inject arbitrary web script or HTML via the lastname parameter.	6.1	More Details
CVE-2021-27317	Cross Site Scripting (XSS) vulnerability in contactus.php in Doctor Appointment System 1.0 allows remote attackers to inject arbitrary web script or HTML via the comment parameter.	6.1	More Details
CVE-2021-26903	LMA ISIDA Retriever 5.2 is vulnerable to XSS via query['text'].	6.1	More Details
CVE-2021-27888	ZendTo before 6.06-4 Beta allows XSS during the display of a drop-off in which a filename has unexpected characters.	6.1	More Details
CVE-2021-26702	EPrints 3.4.2 exposes a reflected XSS opportunity in the dataset parameter to the cgi/dataset_dictionary URI.	6.1	More Details
CVE-2021-20660	Cross-site scripting vulnerability in SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-21308	PrestaShop is a fully scalable open source e-commerce solution. In PrestaShop before version 1.7.2 the soft logout system is not complete and an attacker is able to foreign request and executes customer commands. The problem is fixed in 1.7.7.2	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26475	EPrints 3.4.2 exposes a reflected XSS opportunity in the via a cgi/cal URI.	6.1	More Details
CVE-2021-23974	The DOMParser API did not properly process '<noscript>' elements for escaping. This could be used as an mXSS vector to bypass an HTML Sanitizer. This vulnerability affects Firefox < 86.	6.1	More Details
CVE-2019-18943	Micro Focus Solutions Business Manager versions prior to 11.7.1 are vulnerable to XML External Entity Processing (XXE) on certain operations.	6.1	More Details
CVE-2020-1936	A cross-site scripting issue was found in Apache Ambari Views. This was addressed in Apache Ambari 2.7.4.	6.1	More Details
CVE-2021-27671	An issue was discovered in the comrak crate before 0.9.1 for Rust. XSS can occur because the protection mechanism for data: and javascript: URIs is case-sensitive, allowing (for example) Data: to be used in an attack.	6.1	More Details
CVE-2021-23959	An XSS bug in internal error pages could have led to various spoofing attacks, including other error pages and the address bar. Note: This issue only affected Firefox for Android. Other operating systems are unaffected. This vulnerability affects Firefox < 85.	6.1	More Details
CVE-2021-1724	Microsoft Dynamics Business Central Cross-site Scripting Vulnerability	6.1	More Details
CVE-2021-23955	The browser could have been confused into transferring a pointer lock state into another tab, which could have lead to clickjacking attacks. This vulnerability affects Firefox < 85.	6.1	More Details
CVE-2021-27330	Triconsole Datepicker Calendar <3.77 is affected by cross-site scripting (XSS) in calendar_form.php. Attackers can read authentication cookies that are still active, which can be used to perform further attacks such as reading browser history, directory listings, and file contents.	6.1	More Details
CVE-2020-25902	Blackboard Collaborate Ultra 20.02 is affected by a cross-site scripting (XSS) vulnerability. The XSS payload will execute on the class room, which leads to stealing cookies from users who join the class. NOTE: Third-parties dispute the validity of this entry as a possible false positive during research	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27731	Accellion FTA 9_12_432 and earlier is affected by stored XSS via a crafted POST request to a user endpoint. The fixed version is FTA_9_12_444 and later.	6.1	More Details
CVE-2020-28972	In SaltStack Salt before 3002.5, authentication to VMware vcenter, vsphere, and esxi servers (in the vmware.py files) does not always validate the SSL/TLS certificate.	5.9	More Details
CVE-2021-1229	A vulnerability in ICMP Version 6 (ICMPv6) processing in Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a slow system memory leak, which over time could lead to a denial of service (DoS) condition. This vulnerability is due to improper error handling when an IPv6-configured interface receives a specific type of ICMPv6 packet. An attacker could exploit this vulnerability by sending a sustained rate of crafted ICMPv6 packets to a local IPv6 address on a targeted device. A successful exploit could allow the attacker to cause a system memory leak in the ICMPv6 process on the device. As a result, the ICMPv6 process could run out of system memory and stop processing traffic. The device could then drop all ICMPv6 packets, causing traffic instability on the device. Restoring device functionality would require a device reboot.	5.8	More Details
CVE-2021-21255	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI version 9.5.3, it was possible to switch entities with IDOR from a logged in user. This is fixed in version 9.5.4.	5.8	More Details
CVE-2020-12529	An issue was discovered in MB connect line mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2 There is a SSRF in the LDAP access check, allowing an attacker to scan for open ports.	5.8	More Details
CVE-2021-24114	Microsoft Teams iOS Information Disclosure Vulnerability	5.7	More Details
CVE-2021-1731	PFX Encryption Security Feature Bypass Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1450	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. To exploit this vulnerability, the attacker would need to have valid credentials on the device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending one or more crafted IPC messages to the AnyConnect process on an affected device. A successful exploit could allow the attacker to stop the AnyConnect process, causing a DoS condition on the device. Note: The process under attack will automatically restart so no action is needed by the user or admin.	5.5	More Details
CVE-2021-24084	Windows Mobile Device Management Information Disclosure Vulnerability	5.5	More Details
CVE-2021-24106	Windows DirectX Information Disclosure Vulnerability	5.5	More Details
CVE-2021-24079	Windows Backup Engine Information Disclosure Vulnerability	5.5	More Details
CVE-2021-24076	Microsoft Windows VMSwitch Information Disclosure Vulnerability	5.5	More Details
CVE-2020-27618	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid multi-byte input sequences in IBM1364, IBM1371, IBM1388, IBM1390, and IBM1399 encodings, fails to advance the input state, which could lead to an infinite loop in applications, resulting in a denial of service, a different vulnerability from CVE-2016-10228.	5.5	More Details
CVE-2020-9479	When loading a UDF, a specially crafted zip file could allow files to be placed outside of the UDF deployment directory. This issue affected Apache AsterixDB unreleased builds between commits 580b81aa5e8888b8e1b0620521a1c9680e54df73 and 28c0ee84f1387ab5d0659e9e822f4e3923ddc22d. Note: this CVE may be REJECTed as the issue did not affect any released versions of Apache AsterixDB	5.5	More Details
CVE-2021-22296	A component of HarmonyOS 2.0 has a DoS vulnerability. Local attackers may exploit this vulnerability to mount a file system to the target device, causing DoS of the file system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-18942	Micro Focus Solutions Business Manager versions prior to 11.7.1 are vulnerable to stored XSS. The application reflects previously stored user input without encoding.	5.5	More Details
CVE-2021-27904	An issue was discovered in app/Model/SharingGroupServer.php in MISP 2.4.139. In the implementation of Sharing Groups, the "all org" flag sometimes provided view access to unintended actors.	5.5	More Details
CVE-2021-24098	Windows Console Driver Denial of Service Vulnerability	5.5	More Details
CVE-2021-21622	Jenkins Artifact Repository Parameter Plugin 1.0.0 and earlier does not escape parameter names and descriptions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	5.4	More Details
CVE-2021-3124	Stored cross-site scripting (XSS) in form field in robust.systems product Custom Global Variables v 1.0.5 allows a remote attacker to inject arbitrary code via the vars[0][name] field.	5.4	More Details
CVE-2021-27225	In Dataiku DSS before 8.0.6, insufficient access control in the Jupyter notebooks integration allows users (who have coding permissions) to read and overwrite notebooks in projects that they are not authorized to access.	5.4	More Details
CVE-2021-3151	i-doit before 1.16.0 is affected by Stored Cross-Site Scripting (XSS) issues that could allow remote authenticated attackers to inject arbitrary web script or HTML via C__MONITORING__CONFIG__TITLE, SM2__C__MONITORING__CONFIG__TITLE, C__MONITORING__CONFIG__PATH, SM2__C__MONITORING__CONFIG__PATH, C__MONITORING__CONFIG__ADDRESS, or SM2__C__MONITORING__CONFIG__ADDRESS.	5.4	More Details
CVE-2021-1730	A spoofing vulnerability exists in Microsoft Exchange Server which could result in an attack that would allow a malicious actor to impersonate the user. This update addresses this vulnerability. To prevent these types of attacks, Microsoft recommends customers to download inline images from different DNSdomains than the rest of OWA. Please see further instructions in the FAQ to put in place this mitigations.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21619	Jenkins Claim Plugin 2.18.1 and earlier does not escape the user display name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers who are able to control the display names of Jenkins users, either via the security realm, or directly inside Jenkins.	5.4	More Details
CVE-2021-21618	Jenkins Repository Connector Plugin 2.0.2 and earlier does not escape parameter names and descriptions for past builds, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2021-3355	A stored-self XSS exists in LightCMS v1.3.4, allowing an attacker to execute HTML or JavaScript code in a vulnerable Title field to /admin/SensitiveWords.	5.4	More Details
CVE-2021-20657	Improper access control vulnerability in SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an authenticated attacker to obtain and/or alter the setting information without the access privilege via unspecified vectors.	5.4	More Details
CVE-2021-24113	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	5.4	More Details
CVE-2020-23518	Cross Site Scripting (XSS) vulnerability in UltimateKode Neo Billing - Accounting, Invoicing And CRM Software up to version 3.5 which allows remote attackers to inject arbitrary web script or HTML.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21309	Redis is an open-source, in-memory database that persists on disk. In affected versions of Redis an integer overflow bug in 32-bit Redis version 4.0 or newer could be exploited to corrupt the heap and potentially result with remote code execution. Redis 4.0 or newer uses a configurable limit for the maximum supported bulk input size. By default, it is 512MB which is a safe value for all platforms. If the limit is significantly increased, receiving a large request from a client may trigger several integer overflow scenarios, which would result with buffer overflow and heap corruption. We believe this could in certain conditions be exploited for remote code execution. By default, authenticated Redis users have access to all configuration parameters and can therefore use the “CONFIG SET proto-max-bulk-len” to change the safe default, making the system vulnerable. **This problem only affects 32-bit Redis (on a 32-bit system, or as a 32-bit executable running on a 64-bit system).** The problem is fixed in version 6.2, and the fix is back ported to 6.0.11 and 5.0.11. Make sure you use one of these versions if you are running 32-bit Redis. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent clients from directly executing `CONFIG SET`: Using Redis 6.0 or newer, ACL configuration can be used to block the command. Using older versions, the `rename-command` configuration directive can be used to rename the command to a random string unknown to users, rendering it inaccessible. Please note that this workaround may have an additional impact on users or operational systems that expect `CONFIG SET` to behave in certain ways.	5.4	More Details
CVE-2021-3010	There are multiple persistent cross-site scripting (XSS) vulnerabilities in the web interface of OpenText Content Server Version 20.3. The application allows a remote attacker to introduce arbitrary JavaScript by crafting malicious form values that are later not sanitized.	5.4	More Details
CVE-2021-22114	Addresses partial fix in CVE-2018-1263. Spring-integration-zip, versions prior to 1.0.4, exposes an arbitrary file write vulnerability, that can be achieved using a specially crafted zip archive (affects other archives as well, bzip2, tar, xz, war, cpio, 7z), that holds path traversal filenames. So when the filename gets concatenated to the target extraction directory, the final path ends up outside of the target folder.	5.3	More Details
CVE-2021-21973	The vSphere Client (HTML5) contains an SSRF (Server Side Request Forgery) vulnerability due to improper validation of URLs in a vCenter Server plugin. A malicious actor with network access to port 443 may exploit this issue by sending a POST request to vCenter Server plugin leading to information disclosure. This affects: VMware vCenter Server (7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2 and 3.x before 3.10.1.2).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21328	Vapor is a web framework for Swift. In Vapor before version 4.40.1, there is a DoS attack against anyone who Bootstraps a metrics backend for their Vapor app. The following is the attack vector: 1. send unlimited requests against a vapor instance with different paths. this will create unlimited counters and timers, which will eventually drain the system. 2. downstream services might suffer from this attack as well by being spammed with error paths. This has been patched in 4.40.1. The `DefaultResponder` will rewrite any undefined route paths for to `vapor_route_undefined` to avoid unlimited counters.	5.3	More Details
CVE-2021-24071	Microsoft SharePoint Information Disclosure Vulnerability	5.3	More Details
CVE-2021-23345	All versions of package github.com/thecodingmachine/gotenberg are vulnerable to Server-side Request Forgery (SSRF) via the /convert/html endpoint when the src attribute of an HTML element refers to an internal system file, such as <iframe src='file:///etc/passwd'>.	5.3	More Details
CVE-2021-3384	A vulnerability in Stormshield Network Security could allow an attacker to trigger a protection related to ARP/NDP tables management, which would temporarily prevent the system to contact new hosts via IPv4 or IPv6. This affects versions 2.0.0 to 2.7.7, 2.8.0 to 2.16.0, 3.0.0 to 3.7.16, 3.8.0 to 3.11.4, and 4.0.0 to 4.1.5. Fixed in versions 2.7.8, 3.7.17, 3.11.5, and 4.2.0.	5.3	More Details
CVE-2020-36240	The ResourceDownloadRewriteRule class in Crowd before version 4.0.4, and from version 4.1.0 before 4.1.2 allowed unauthenticated remote attackers to read arbitrary files within WEB-INF and META-INF directories via an incorrect path access check.	5.3	More Details
CVE-2020-27223	In Eclipse Jetty 9.4.6.v20170531 to 9.4.36.v20210114 (inclusive), 10.0.0, and 11.0.0 when Jetty handles a request containing multiple Accept headers with a large number of “quality” (i.e. q) parameters, the server may enter a denial of service (DoS) state due to high CPU usage processing those quality values, resulting in minutes of CPU time exhausted processing those quality values.	5.3	More Details
CVE-2021-21621	Jenkins Support Core Plugin 2.72 and earlier provides the serialized user authentication as part of the "About user (basic authentication details only)" information, which can include the session ID of the user creating the support bundle in some configurations.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3332	WPS Hide Login 1.6.1 allows remote attackers to bypass a protection mechanism via post_password.	5.3	More Details
CVE-2021-23977	Firefox for Android suffered from a time-of-check-time-of-use vulnerability that allowed a malicious application to read sensitive data from application directories. Note: This issue is only affected Firefox for Android. Other operating systems are unaffected. This vulnerability affects Firefox < 86.	5.3	More Details
CVE-2021-27884	Weak JSON Web Token (JWT) signing secret generation in YMFE YApi through 1.9.2 allows recreation of other users' JWT tokens. This occurs because Math.random in Node.js is used.	5.1	More Details
CVE-2021-24100	Microsoft Edge for Android Information Disclosure Vulnerability	5.0	More Details
CVE-2019-18944	Micro Focus Solutions Business Manager Application Repository versions prior to 11.7.1 are vulnerable to reflected XSS.	4.9	More Details
CVE-2018-25004	A user authorized to performing a specific type of query may trigger a denial of service by issuing a generic explain command on a find query. This issue affects MongoDB Server v4.0 versions prior to 4.0.6 and MongoDB Server v3.6 versions prior to 3.6.11.	4.9	More Details
CVE-2020-4719	The IBM Cloud APM 8.1.4 server will issue a DNS request to resolve any hostname specified in the Cloud Event Management Webhook URL configuration definition. This could enable an authenticated user with admin authorization to create DNS query strings that are not hostnames. IBM X-Force ID: 187861.	4.9	More Details
CVE-2021-21514	Dell EMC OpenManage Server Administrator (OMSA) versions 9.5 and prior contain a path traversal vulnerability. A remote user with admin privileges could potentially exploit this vulnerability to view arbitrary files on the target system by sending a specially crafted URL request.	4.9	More Details
CVE-2019-18946	Micro Focus Solutions Business Manager Application Repository versions prior to 11.7.1 are vulnerable to session fixation.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1231	A vulnerability in the Link Layer Discovery Protocol (LLDP) for Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an unauthenticated, adjacent attacker to disable switching on a small form-factor pluggable (SFP) interface. This vulnerability is due to incomplete validation of the source of a received LLDP packet. An attacker could exploit this vulnerability by sending a crafted LLDP packet on an SFP interface to an affected device. A successful exploit could allow the attacker to disable switching on the SFP interface, which could disrupt network traffic.	4.7	More Details
CVE-2021-21616	Jenkins Active Choices Plugin 2.5.2 and earlier does not escape reference parameter values, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	4.6	More Details
CVE-2020-12702	Weak encryption in the Quick Pairing mode in the eWeLink mobile application (Android application V4.9.2 and earlier, iOS application V4.9.1 and earlier) allows physically proximate attackers to eavesdrop on Wi-Fi credentials and other sensitive information by monitoring the Wi-Fi spectrum during the pairing process.	4.6	More Details
CVE-2021-0403	In netdiag, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05475124.	4.4	More Details
CVE-2021-0404	In mobile_log_d, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05457039.	4.4	More Details
CVE-2021-21724	A ZTE product has a memory leak vulnerability. Due to the product's improper handling of memory release in certain scenarios, a local attacker with device permissions repeatedly attenuated the optical signal to cause memory leak and abnormal service. This affects: ZXR10 8900E, all versions up to V3.03.20R2B30P1.	4.4	More Details
CVE-2021-25284	An issue was discovered in through SaltStack Salt before 3002.5. salt.modules.cmdmod can log credentials to the info or error log level.	4.4	More Details
CVE-2021-22187	An issue has been discovered in GitLab affecting all versions of Gitlab EE/CE before 13.6.7. A potential resource exhaustion issue that allowed running or pending jobs to continue even after project was deleted.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20656	Exposure of information through directory listing in SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an authenticated attacker to obtain the information inside the system, such as directories and/or file configurations via unspecified vectors.	4.3	More Details
CVE-2021-21274	Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.25.0, a malicious homeserver could redirect requests to their .well-known file to a large file. This can lead to a denial of service attack where homeservers will consume significantly more resources when requesting the .well-known file of a malicious homeserver. This affects any server which accepts federation requests from untrusted servers. Issue is resolved in version 1.25.0. As a workaround the `federation_domain_whitelist` setting can be used to restrict the homeservers communicated with over federation.	4.3	More Details
CVE-2020-12530	An issue was discovered in MB connect line mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. There is an XSS issue in the redirect.php allowing an attacker to inject code via a get parameter.	4.3	More Details
CVE-2021-23968	If Content Security Policy blocked frame navigation, the full destination of a redirect served in the frame was reported in the violation report; as opposed to the original frame URI. This could be used to leak sensitive information contained in such URIs. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.	4.3	More Details
CVE-2021-21620	A cross-site request forgery (CSRF) vulnerability in Jenkins Claim Plugin 2.18.1 and earlier allows attackers to change claims.	4.3	More Details
CVE-2021-1367	A vulnerability in the Protocol Independent Multicast (PIM) feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted PIM packet to an affected device. A successful exploit could allow the attacker to cause a traffic loop, resulting in a DoS condition.	4.3	More Details
CVE-2021-23963	When sharing geolocation during an active WebRTC share, Firefox could have reset the webRTC sharing state in the user interface, leading to loss of control over the currently granted permission. This vulnerability affects Firefox < 85.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23953	If a user clicked into a specifically crafted PDF, the PDF reader could be confused into leaking cross-origin information, when said information is served as chunked data. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.	4.3	More Details
CVE-2021-23969	As specified in the W3C Content Security Policy draft, when creating a violation report, "User agents need to ensure that the source file is the URL requested by the page, pre-redirects. If that’s not possible, user agents need to strip the URL down to an origin to avoid unintentional leakage." Under certain types of redirects, Firefox incorrectly set the source file to be the destination of the redirects. This was fixed to be the redirect destination's origin. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.	4.3	More Details
CVE-2021-24082	Microsoft.PowerShell.Utility Module WDAC Security Feature Bypass Vulnerability	4.3	More Details
CVE-2021-21298	Node-Red is a low-code programming for event-driven applications built using nodejs. Node-RED 1.2.7 and earlier has a vulnerability which allows arbitrary path traversal via the Projects API. If the Projects feature is enabled, a user with `projects.read` permission is able to access any file via the Projects API. The issue has been patched in Node-RED 1.2.8. The vulnerability applies only to the Projects feature which is not enabled by default in Node-RED. The primary workaround is not give untrusted users read access to the Node-RED editor.	3.5	More Details
CVE-2019-18947	Micro Focus Solutions Business Manager Application Repository versions prior to 11.7.1 are vulnerable to information disclosure.	3.5	More Details
CVE-2020-4725	IBM Monitoring (IBM Cloud APM 8.1.4) could allow an authenticated user to modify HTML content by sending a specially crafted HTTP request to the APM UI, which could mislead another user. IBM X-Force ID: 187974.	3.5	More Details
CVE-2021-22294	A component API of the HarmonyOS 2.0 has a permission bypass vulnerability. Local attackers may exploit this vulnerability to issue commands repeatedly, exhausting system service resources.	3.3	More Details
CVE-2020-4726	The IBM Application Performance Monitoring UI (IBM Cloud APM 8.1.4) allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 187975.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20203	An integer overflow issue was found in the vmxnet3 NIC emulator of the QEMU for versions up to v5.2.0. It may occur if a guest was to supply invalid values for rx/tx queue size or other NIC parameters. A privileged guest user may use this flaw to crash the QEMU process on the host resulting in DoS scenario.	3.2	More Details
CVE-2021-21273	Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.25.0, requests to user provided domains were not restricted to external IP addresses when calculating the key validity for third-party invite events and sending push notifications. This could cause Synapse to make requests to internal infrastructure. The type of request was not controlled by the user, although limited modification of request bodies was possible. For the most thorough protection server administrators should remove the deprecated `federation_ip_range_blacklist` from their settings after upgrading to Synapse v1.25.0 which will result in Synapse using the improved default IP address restrictions. See the new `ip_range_blacklist` and `ip_range_whitelist` settings if more specific control is necessary.	3.1	More Details
CVE-2021-21330	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. In aiohttp before version 3.7.4 there is an open redirect vulnerability. A maliciously crafted link to an aiohttp-based web-server could redirect the browser to a different website. It is caused by a bug in the `aiohttp.web_middlewares.normalize_path_middleware` middleware. This security problem has been fixed in 3.7.4. Upgrade your dependency using pip as follows "pip install aiohttp >= 3.7.4". If upgrading is not an option for you, a workaround can be to avoid using `aiohttp.web_middlewares.normalize_path_middleware` in your applications.	3.1	More Details
CVE-2021-21320	matrix-react-sdk is an npm package which is a Matrix SDK for React Javascript. In matrix-react-sdk before version 3.15.0, the user content sandbox can be abused to trick users into opening unexpected documents. The content is opened with a `blob` origin that cannot access Matrix user data, so messages and secrets are not at risk. This has been fixed in version 3.15.0.	2.6	More Details
CVE-2021-27645	The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.	2.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-3633	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2016-8154	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8142	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8143	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8144	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8145	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8146	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8147	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8148	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8149	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8150	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8151	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8152	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8153	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8155	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2021-21065	Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2016-8156	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8157	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8158	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8159	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8160	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8003	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8001	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8140	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2020-9051	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-9052	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-9053	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21064	Magento UPWARD-php version 1.1.4 (and earlier) is affected by a Path traversal vulnerability in Magento UPWARD Connector version 1.1.2 (and earlier) due to the upload feature. An attacker could potentially exploit this vulnerability to upload a malicious YAML file that can contain instructions which allows reading arbitrary files from the remote server. Access to the admin console is required for successful exploitation.	N/A	More Details
CVE-2016-8141	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8004	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8013	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8047	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8113	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8112	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8111	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8110	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8109	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8108	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8107	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8049	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8048	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8046	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8115	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8045	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8044	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8043	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8042	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8041	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8040	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8028	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8015	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8014	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8114	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8116	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8138	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8128	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8137	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8136	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8135	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8134	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8133	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8132	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8131	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8130	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8129	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8127	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8117	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8126	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8125	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8124	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8123	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8122	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8121	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8120	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8119	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8118	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details
CVE-2016-8139	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2016. Notes: none	N/A	More Details