SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 17 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-2021-26867	Windows Hyper-V Remote Code Execution Vulnerability	9.9	More Details
CVE-2020-24791	FUEL CMS 1.4.8 allows SQL injection via the 'fuel_replace_id' parameter in pages/replace/1. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.	9.8	More Details
CVE-2021-20231	A flaw was found in gnutls. A use after free issue in client sending key_share extension may lead to memory corruption and other consequences.	9.8	More Details
CVE-2016-20009	A DNS client stack-based buffer overflow in ipdnsc_decode_name() affects Wind River VxWorks 6.5 through 7. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36282	JMS Client for RabbitMQ 1.x before 1.15.2 and 2.x before 2.2.0 is vulnerable to unsafe deserialization that can result in code execution via crafted StreamMessage data.	9.8	More Details
CVE-2021-26569	Race Condition within a Thread vulnerability in iscsi_snapshot_comm_core in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via crafted web requests.	9.8	More Details
CVE-2021-27646	Use After Free vulnerability in iscsi_snapshot_comm_core in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via crafted web requests.	9.8	More Details
CVE-2021-27647	Out-of-bounds Read vulnerability in iscsi_snapshot_comm_core in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via crafted web requests.	9.8	More Details
CVE-2021-28305	An issue was discovered in the diesel crate before 1.4.6 for Rust. There is a use-after-free in the SQLite backend because the semantics of sqlite3_column_name are not followed.	9.8	More Details
CVE-2021-20232	A flaw was found in gnutls. A use after free issue in client_send_params in lib/ext/pre_shared_key.c may lead to memory corruption and other potential consequences.	9.8	More Details
CVE-2020-29045	The food-and-drink-menu plugin through 2.2.0 for WordPress allows remote attackers to execute arbitrary code because of an unserialize operation on the fdm_cart cookie in load_cart_from_cookie in includes/class-cart-manager.php.	9.8	More Details
CVE-2020-35358	DomainMOD domainmod-v4.15.0 is affected by an insufficient session expiration vulnerability. On changing a password, both sessions using the changed password and old sessions in any other browser or device do not expire and remain active. Such flaws frequently give attackers unauthorized access to some system data or functionality.	9.8	More Details
CVE-2020-24877	A SQL injection vulnerability in zzzphp v1.8.0 through /form/index.php?module=getjson may lead to a possible access restriction bypass.	9.8	More Details
CVE-2021-27817	A remote command execution vulnerability in shopxo 1.9.3 allows an attacker to upload malicious code generated by phar where the suffix is JPG, which is uploaded after modifying the phar suffix.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26987	Element Plug-in for vCenter Server incorporates SpringBoot Framework. SpringBoot Framework versions prior to 1.3.2 are susceptible to a vulnerability which when successfully exploited could lead to Remote Code Execution. All versions of Element Plug-in for vCenter Server, Management Services versions prior to 2.17.56 and Management Node versions through 12.2 contain vulnerable versions of SpringBoot Framework.	9.8	More Details
CVE-2020-24264	Portainer 1.24.1 and earlier is affected by incorrect access control that may lead to remote arbitrary code execution. The restriction checks for bind mounts are applied only on the client-side and not the server-side, which can lead to spawning a container with bind mount. Once such a container is spawned, it can be leveraged to break out of the container leading to complete Docker host machine takeover.	9.8	More Details
CVE-2021-25916	Prototype pollution vulnerability in 'patchmerge' versions 1.0.0 through 1.0.1 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2021-28294	Online Ordering System 1.0 is vulnerable to arbitrary file upload through /onlineordering/GPST/store/initiateorder.php, which may lead to remote code execution (RCE).	9.8	More Details
CVE-2021-28122	A request-validation issue was discovered in Open5GS 2.1.3 through 2.2.x before 2.2.1. The WebUI component allows an unauthenticated user to use a crafted HTTP API request to create, read, update, or delete entries in the subscriber database. For example, new administrative users can be added. The issue occurs because Express is not set up to require authentication.	9.8	More Details
CVE-2021-22714	A CWE-119:Improper restriction of operations within the bounds of a memory buffer vulnerability exists in PowerLogic ION7400, PM8000 and ION9000 (All versions prior to V3.0.0), which could cause the meter to reboot or allow for remote code execution.	9.8	More Details
CVE-2021-28141	An issue was discovered in Progress Telerik UI for ASP.NET AJAX 2021.1.224. It allows unauthorized access to MicrosoftAjax.js through the Telerik.Web.UI.WebResource.axd file. This may allow the attacker to gain unauthorized access to the server and execute code. To exploit, one must use the parameter _TSM_HiddenField_ and inject a command at the end of the URI. NOTE: the vendor states that this is not a vulnerability. The request's output does not indicate that a "true" command was executed on the server, and the request's output does not leak any private source code or data from the server	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28132	LUCY Security Awareness Software through 4.7.x allows unauthenticated remote code execution because the Migration Tool (in the Support section) allows upload of .php files within a system.tar.gz file. The .php file becomes accessible with a public/system/static URI.	9.8	More Details
CVE-2020-1916	An incorrect size calculation in ldap_escape may lead to an integer overflow when overly long input is passed in, resulting in an out-of-bounds write. This issue affects HHVM prior to 4.56.2, all versions between 4.57.0 and 4.78.0, 4.79.0, 4.80.0, 4.81.0, 4.82.0, 4.83.0.	9.8	More Details
CVE-2020-1917	xbuf_format_converter, used as part of exif_read_data, was appending a terminating null character to the generated string, but was not using its standard append char function. As a result, if the buffer was full, it would result in an out-of-bounds write. This issue affects HHVM versions prior to 4.56.3, all versions between 4.57.0 and 4.80.1, all versions between 4.81.0 and 4.93.1, and versions 4.94.0, 4.95.0, 4.96.0, 4.97.0, 4.98.0.	9.8	More Details
CVE-2021-0396	In Builtins::Generate_ArgumentsAdaptorTrampoline of builtins-arm.cc and related files, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-160610106	9.8	More Details
CVE-2021-0397	In sdp_copy_raw_data of sdp_discovery.cc, there is a possible system compromise due to a double free. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174052148	9.8	More Details
CVE-2021-24025	Due to incorrect string size calculations inside the preg_quote function, a large input string passed to the function can trigger an integer overflow leading to a heap overflow. This issue affects HHVM versions prior to 4.56.3, all versions between 4.57.0 and 4.80.1, all versions between 4.81.0 and 4.93.1, and versions 4.94.0, 4.95.0, 4.96.0, 4.97.0, 4.98.0.	9.8	More Details
CVE-2021-24030	The fbgames protocol handler registered as part of Facebook Gameroom does not properly quote arguments passed to the executable. That allows a malicious URL to cause code execution. This issue affects versions prior to v1.26.0.	9.8	More Details
CVE-2021-28134	Clipper before 1.0.5 allows remote command execution. A remote attacker may send a crafted IPC message to the exposed vulnerable ipcRenderer IPC interface, which invokes the dangerous openExternal API.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1900	When unserializing an object with dynamic properties HHVM needs to pre-reserve the full size of the dynamic property array before inserting anything into it. Otherwise the array might resize, invalidating previously stored references. This pre-reservation was not occurring in HHVM prior to v4.32.3, between versions 4.33.0 and 4.56.0, 4.57.0, 4.58.0, 4.58.1, 4.59.0, 4.60.0, 4.61.0, 4.62.0.	9.8	More Details
CVE-2021-26877	Windows DNS Server Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-26893	Windows DNS Server Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-26894	Windows DNS Server Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-26895	Windows DNS Server Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-26897	Windows DNS Server Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-28381	The vhs (aka VHS: Fluid ViewHelpers) extension before 5.1.1 for TYPO3 allows SQL injection via isLanguageViewHelper.	9.8	More Details
CVE-2020-28149	myDBR 5.8.3/4262 is affected by: Cross Site Scripting (XSS). The impact is: execute arbitrary code (remote). The component is: CSRF Token. The attack vector is: CSRF token injection to XSS.	9.6	More Details
CVE-2021-27080	Azure Sphere Unsigned Code Execution Vulnerability	9.3	More Details
CVE-2021-28308	An issue was discovered in the fltk crate before 0.15.3 for Rust. There is an out-of bounds read because the pixmap constructor lacks pixmap input validation.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28899	The Web CGI Script on ZyXEL LTE4506-M606 V1.00(ABDO.2)C0 devices does not require authentication, which allows remote unauthenticated attackers (via crafted JSON action data to /cgi-bin/gui.cgi) to use all features provided by the router. Examples: change the router password, retrieve the Wi-Fi passphrase, send an SMS message, or modify the IP forwarding to access the internal network.	9.1	More Details
CVE-2021-28154	Camunda Modeler (aka camunda-modeler) through 4.6.0 allows arbitrary file access. A remote attacker may send a crafted IPC message to the exposed vulnerable ipcRenderer IPC interface, which manipulates the readFile and writeFile APIs. NOTE: the vendor states "The way we secured the app is that it does not allow any remote scripts to be opened, no unsafe scripts to be evaluated, no remote sites to be browsed.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-3344	A privilege escalation flaw was found in OpenShift builder. During build time, credentials outside the build context are automatically mounted into the container image under construction. An OpenShift user, able to execute code during build time inside this container can re-use the credentials to overwrite arbitrary container images in internal registries and/or escalate their privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This affects github.com/openshift/builder v0.0.0-20210125201112-7901cb396121 and before.	8.8	More Details
CVE-2020-24983	An issue was discovered in Quadbase EspressReports ES 7 Update 9. An unauthenticated attacker can create a malicious HTML file that houses a POST request made to the DashboardBuilder within the target web application. This request will utilise the target admin session and perform the authenticated request (to change the Dashboard name) as if the victim had done so themselves, aka CSRF.	8.8	More Details
CVE-2020-35231	The NSDP protocol implementation on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices was affected by an authentication issue that allows an attacker to bypass access controls and obtain full control of the device.	8.8	More Details
CVE-2021-28144	prog.cgi on D-Link DIR-3060 devices before 1.11b04 HF2 allows remote authenticated users to inject arbitrary commands in an admin or root context because SetVirtualServerSettings calls CheckArpTables, which calls popen unsafely.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25672	A vulnerability has been identified in Mendix Forgot Password Appstore module (All Versions < V3.2.1). The Forgot Password Marketplace module does not properly control access. An attacker could take over accounts.	8.8	More Details
CVE-2021-25667	A vulnerability has been identified in RUGGEDCOM RM1224 (All versions >= V4.3 and < V6.4), SCALANCE M-800 (All versions >= V4.3 and < V6.4), SCALANCE S615 (All versions >= V4.3 and < V6.4), SCALANCE SC-600 Family (All versions >= V2.0 and < V2.1.3), SCALANCE XB-200 (All versions < V4.1), SCALANCE XC-200 (All versions < V4.1), SCALANCE XF-200BA (All versions < V4.1), SCALANCE XM400 (All versions < V6.2), SCALANCE XP-200 (All versions < V4.1), SCALANCE XR-300WG (All versions < V4.1), SCALANCE XR500 (All versions < V6.2). Affected devices contain a stack-based buffer overflow vulnerability in the handling of STP BPDU frames that could allow a remote attacker to trigger a denial-of-service condition or potentially remote code execution. Successful exploitation requires the passive listening feature of the device to be active.	8.8	More Details
CVE-2020-35229	The authentication token required to execute NSDP write requests on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices is not properly invalidated and can be reused until a new token is generated, which allows attackers (with access to network traffic) to effectively gain administrative privileges.	8.8	More Details
CVE-2020-35223	The CSRF protection mechanism implemented in the web administration panel on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices could be bypassed by omitting the CSRF token parameter in HTTP requests.	8.8	More Details
CVE-2020-25240	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0). Unpriviledged users can access services when guessing the url. An attacker could impact availability, integrity and gain information from logs and templates of the service.	8.8	More Details
CVE-2021-28379	web/upload/UploadHandler.php in Vesta Control Panel (aka VestaCP) through 0.9.8-27 and myVesta through 0.9.8-26-39 allows uploads from a different origin.	8.8	More Details
CVE-2020-25239	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0). The webserver could allow unauthorized actions via special urls for unpriviledged users. The settings of the UMC authorization server could be changed to add a rogue server by an attacker authenticating with unprivilege user rights.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35221	The hashing algorithm implemented for NSDP password authentication on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices was found to be insecure, allowing attackers (with access to a network capture) to quickly generate multiple collisions to generate valid passwords, or infer some parts of the original.	8.8	More Details
CVE-2020-24984	An issue was discovered in Quadbase EspressReports ES 7 Update 9. It allows CSRF, whereby an attacker may be able to trick an authenticated admin level user into uploading malicious files to the web server.	8.8	More Details
CVE-2021-27891	SSH Tectia Client and Server before 6.4.19 on Windows have weak key generation. ConnectSecure on Windows is affected.	8.8	More Details
CVE-2020-19417	Emerson Smart Wireless Gateway 1420 4.6.59 allows non-privileged users (such as the default account 'maint') to perform administrative tasks by sending specially crafted HTTP requests to the application.	8.8	More Details
CVE-2021-20017	A post-authenticated command injection vulnerability in SonicWall SMA100 allows an authenticated attacker to execute OS commands as a 'nobody' user. This vulnerability impacts SMA100 version 10.2.0.5 and earlier.	8.8	More Details
CVE-2021-27085	Internet Explorer Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-27076	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-26411	Internet Explorer Memory Corruption Vulnerability	8.8	More Details
CVE-2021-27890	SQL Injection vulnerablity in MyBB before 1.8.26 via theme properties included in theme XML files.	8.8	More Details
CVE-2020-23722	An issue was discovered in FUEL CMS 1.4.7. There is a escalation of privilege vulnerability to obtain super admin privilege via the "id" and "fuel_id" parameters.	8.8	More Details
CVE-2021-27946	SQL Injection vulnerability in MyBB before 1.8.26 via poll vote count. (issue 1 of 3).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29553	The Scheduler in Grav CMS through 1.7.0-rc.17 allows an attacker to execute a system command by tricking an admin into visiting a malicious website (CSRF).	8.8	More Details
CVE-2021-27230	ExpressionEngine before 5.4.2 and 6.x before 6.0.3 allows PHP Code Injection by certain authenticated users who can leverage Translate::save() to write to an _lang.php file under the system/user/language directory.	8.8	More Details
CVE-2020-24263	Portainer 1.24.1 and earlier is affected by an insecure permissions vulnerability that may lead to remote arbitrary code execution. A non-admin user is allowed to spawn new containers with critical capabilities such as SYS_MODULE, which can be used to take over the Docker host.	8.8	More Details
CVE-2021-21191	Use after free in WebRTC in Google Chrome prior to 89.0.4389.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21192	Heap buffer overflow in tab groups in Google Chrome prior to 89.0.4389.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21193	Use after free in Blink in Google Chrome prior to 89.0.4389.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-26865	Windows Container Execution Agent Elevation of Privilege Vulnerability	8.8	More Details
CVE-2021-26876	OpenType Font Parsing Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-13936	An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.	8.8	More Details
CVE-2020-35682	Zoho ManageEngine ServiceDesk Plus before 11134 allows an Authentication Bypass (only during SAML login).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26864	Windows Virtual Registry Provider Elevation of Privilege Vulnerability	8.4	More Details
CVE-2021-21378	Envoy is a cloud-native high-performance edge/middle/service proxy. In Envoy version 1.17.0 an attacker can bypass authentication by presenting a JWT token with an issuer that is not in the provider list when Envoy's JWT Authentication filter is configured with the `allow_missing` requirement under `requires_any` due to a mistake in implementation. Envoy's JWT Authentication filter can be configured with the `allow_missing` requirement that will be satisfied if JWT is missing (JwtMissed error) and fail if JWT is presented or invalid. Due to a mistake in implementation, a JwtUnknownIssuer error was mistakenly converted to JwtMissed when `requires_any` was configured. So if `allow_missing` was configured under `requires_any`, an attacker can bypass authentication by presenting a JWT token with an issuer that is not in the provider list. Integrity may be impacted depending on configuration if the JWT token is used to protect against writes or modifications. This regression was introduced on 2020/11/12 in PR 13839 which fixed handling `allow_missing` under RequiresAny in a JwtRequirement (see issue 13458). The AnyVerifier aggregates the children verifiers' results into a final status where JwtMissing is the default error. However, a JwtUnknownIssuer was mistakenly treated the same as a JwtMissing error and the resulting final aggregation was the default JwtMissing. As a result, `allow_missing` would allow a JWT token with an unknown issuer status. This is fixed in version 1.17.1 by PR 15194. The fix works by preferring JwtUnknownIssuer over a JwtMissing error, fixing the accidental conversion and bypass with `allow_missing`. A user could detect whether a bypass occurred if they have Envoy logs enabled with debug verbosity. Users can enable component level debug logs for JWT. The JWT filter logs will indicate that there is a request with a JWT token and a failure that the JWT token is missing.	8.2	More Details
CVE-2021-21772	A use-after-free vulnerability exists in the NMR::COpcPackageReader::releaseZIP() functionality of 3MF Consortium lib3mf 2.0.0. A specially crafted 3MF file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.1	More Details
CVE-2020-24985	An issue was discovered in Quadbase EspressReports ES 7 Update 9. An authenticated user is able to navigate to the MenuPage section of the application, and change the frmsrc parameter value to retrieve and execute external files or payloads.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29555	The BackupDelete functionality in Grav CMS through 1.7.0-rc.17 allows an authenticated attacker to delete arbitrary files on the underlying server by exploiting a path-traversal technique. (This vulnerability can also be exploited by an unauthenticated attacker due to a lack of CSRF protection.)	8.1	More Details
CVE-2021-20179	A flaw was found in pki-core. An attacker who has successfully compromised a key could use this flaw to renew the corresponding certificate over and over again, as long as it is not explicitly revoked. The highest threat from this vulnerability is to data confidentiality and integrity.	8.1	More Details
CVE-2021-28143	/jsonrpc on D-Link DIR-841 3.03 and 3.04 devices allows authenticated command injection via ping, ping6, or traceroute (under System Tools).	8.0	More Details
CVE-2021-27057	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27051	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27053	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-24090	Windows Error Reporting Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-24089	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27054	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-3310	Western Digital My Cloud OS 5 devices before 5.10.122 mishandle Symbolic Link Following on SMB and AFP shares. This can lead to code execution and information disclosure (by reading local files).	7.8	More Details
CVE-2021-1640	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5025	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 db2fm is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 193661.	7.8	More Details
CVE-2021-27056	Microsoft PowerPoint Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-0391	In onCreate() of ChooseTypeAndAccountActivity.java, there is a possible way to learn the existence of an account, without permissions, due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-172841550	7.8	More Details
CVE-2021-24108	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27058	Microsoft Office ClickToRun Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27060	Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27061	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27062	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27381	A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP3). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds read past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12534)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27077	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-27081	Visual Studio Code ESLint Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27082	Quantum Development Kit for Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27083	Remote Development Extension for Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-0392	In main of main.cpp, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-175124730	7.8	More Details
CVE-2021-27050	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-24110	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-0025	In deletePackageVersionedInternal of PackageManagerService.java, there is a possible way to exit Screen Pinning due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-135604684	7.8	More Details
CVE-2021-26860	Windows App-V Overlay Filter Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26889	Windows Update Stack Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26887	An elevation of privilege vulnerability exists in Microsoft Windows when Folder redirection has been enabled via Group Policy. When folder redirection file server is co-located with Terminal server, an attacker who successfully exploited the vulnerability would be able to begin redirecting another user's personal data to a created folder. To exploit the vulnerability, an attacker can create a new folder under the Folder Redirection root path and create a junction on a newly created User folder. When the new user logs in, Folder Redirection would start redirecting to the folder and copying personal data. This elevation of privilege vulnerability can only be addressed by reconfiguring Folder Redirection with Offline files and restricting permissions, and NOT via a security update for affected Windows Servers. See the FAQ section of this CVE for configuration guidance.	7.8	More Details
CVE-2021-26885	Windows WalletService Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26898	Windows Event Tracing Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26882	Remote Access API Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26899	Windows UPnP Device Host Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26880	Storage Spaces Controller Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26900	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26878	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26875	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26874	Windows Overlay Filter Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26901	Windows Event Tracing Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26872	Windows Event Tracing Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26871	Windows WalletService Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26870	Windows Projected File System Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26902	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-26868	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-27047	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27048	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27049	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-26861	Windows Graphics Component Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27380	A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12532)	7.8	More Details
CVE-2021-27084	Visual Studio Code Java Extension Pack Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-21067	Adobe Photoshop versions 21.2.5 (and earlier) and 22.2 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType library. An unauthenticated attacker could leverage this vulnerability to achieve 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-2021-0385	In createConnectToAvailableNetworkNotification of ConnectToNetworkNotificationBuilder.java, there is a possible connection to untrusted WiFi networks due to notification interaction above the lockscreen. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172584372	7.8	More Details
CVE-2020-28385	A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing DFT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12049)	7.8	More Details
CVE-2021-21082	Adobe Photoshop versions 21.2.5 (and earlier) and 22.2 (and earlier) are affected by a Memory Corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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-2021-21085	Adobe Connect version 11.0.7 (and earlier) is affected by an Input Validation vulnerability in the export feature. An attacker could exploit this vulnerability by injecting a payload into an online event form and achieve code execution if the victim exports and opens the data on their local machine.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21518	Dell SupportAssist Client for Consumer PCs versions 3.7.x, 3.6.x, 3.4.x, 3.3.x, Dell SupportAssist Client for Business PCs versions 2.0.x, 2.1.x, 2.2.x, and Dell SupportAssist Client ProManage 1.x contain a DLL injection vulnerability in the Costura Fody plugin. A local user with low privileges could potentially exploit this vulnerability, leading to the execution of arbitrary executable on the operating system with SYSTEM privileges.	7.8	More Details
CVE-2021-0389	In setNightModeActivated of UiModeManagerService.java, there is a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168039904	7.8	More Details
CVE-2021-0388	In onReceive of ImsPhoneCallTracker.java, there is a possible misattribution of data usage due to an incorrect broadcast handler. This could lead to local escalation of privilege resulting in attributing video call data to the wrong app, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-162741489	7.8	More Details
CVE-2021-0386	In onCreate of UsbConfirmActivity, there is a possible tapjacking vector due to an insecure default value. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-173421110	7.8	More Details
CVE-2021-0383	In done of CaptivePortalLoginActivity.java, there is a confused deputy. This could lead to local escalation of privilege in carrier settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-160871056	7.8	More Details
CVE-2021-0464	In sound_trigger_event_alloc of platform.h, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-167663878	7.8	More Details
CVE-2021-0380	In onReceive of DcTracker.java, there is a possible way to trigger a provisioning URL and modify other telephony settings due to a missing permission check. This could lead to local escalation of privilege during the onboarding flow with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172459128	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28375	An issue was discovered in the Linux kernel through 5.11.6. fastrpc_internal_invoke in drivers/misc/fastrpc.c does not prevent user applications from sending kernel RPC messages, aka CID-20c40794eb85. This is a related issue to CVE-2019-2308.	7.8	More Details
CVE-2021-0390	In various methods of WifiNetworkSuggestionsManager.java, there is a possible modification of suggested networks due to a missing permission check. This could lead to local escalation of privilege by a background user on the same device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174749461	7.8	More Details
CVE-2021-0399	In qtaguid_untag of xt_qtaguid.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-176919394References: Upstream kernel	7.8	More Details
CVE-2021-0398	In bindServiceLocked of ActiveServices.java, there is a possible foreground service launch due to a confused deputy. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-173516292	7.8	More Details
CVE-2021-0395	In StopServicesAndLogViolations of reboot.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-170315126	7.8	More Details
CVE-2021-0393	In Scanner::LiteralBuffer::NewCapacity of scanner.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution if an attacker can supply a malicious PAC file, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-168041375	7.8	More Details
CVE-2021-20674	Untrusted search path vulnerability in Installer of MagicConnect Client program distributed before 2021 March 1 allows an attacker to gain privileges and via a Trojan horse DLL in an unspecified directory and to execute arbitrary code with the privilege of the user invoking the installer when a terminal is connected remotely using Remote desktop.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26890	Application Virtualization Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27892	SSH Tectia Client and Server before 6.4.19 on Windows allow local privilege escalation. ConnectSecure on Windows is affected.	7.8	More Details
CVE-2021-22710	A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could cause remote code execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2021-0372	In getMediaOutputSliceAction of RemoteMediaSlice.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174047735	7.8	More Details
CVE-2021-22712	A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could result in arbitrary read or write conditions when malicious CGF (Configuration Group File) file is imported to IGSS Definition due to an unchecked pointer address.	7.8	More Details
CVE-2021-22711	A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could result in arbitrary read or write conditions when malicious CGF (Configuration Group File) file is imported to IGSS Definition due to missing validation of input data.	7.8	More Details
CVE-2021-26891	Windows Container Execution Agent Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-0376	In checkUriPermission and related functions of MediaProvider.java, there is a possible way to access external files due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-115619667	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22709	A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could result in loss of data or remote code execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2021-0465	In GenerateFaceMask of face.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-172005755	7.8	More Details
CVE-2021-0369	In CrossProfileAppsServiceImpl.java, there is the possibility of an application's INTERACT_ACROSS_PROFILES grant state not displaying properly in the setting UI due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-166561076	7.8	More Details
CVE-2021-21379	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions of XWiki Platform, the `{{wikimacrocontent}}` executes the content with the rights of the wiki macro author instead of the caller of that wiki macro. This makes possible to inject scripts through it and they will be executed with the rights of the wiki macro (very often a user which has Programming rights). Fortunately, no such macro exists by default in XWiki Standard but one could have been created or installed with an extension. This vulnerability has been patched in versions XWiki 12.6.3, 11.10.11 and 12.8-rc-1. There is no easy workaround other than disabling the affected macros. Inserting content in a safe way or knowing what is the user who called the wiki macro is not easy.	7.7	More Details
CVE-2021-26859	Microsoft Power BI Information Disclosure Vulnerability	7.7	More Details
CVE-2021-27059	Microsoft Office Remote Code Execution Vulnerability	7.6	More Details
CVE-2021-26896	Windows DNS Server Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25241	A vulnerability has been identified in SIMATIC MV400 family (All Versions < V7.0.6). The underlying TCP stack of the affected products does not correctly validate the sequence number for incoming TCP RST packages. An attacker could exploit this to terminate arbitrary TCP sessions.	7.5	More Details
CVE-2021-27576	If was found that the NetTest web service can be used to overload the bandwidth of a Apache OpenMeetings server. This issue was addressed in Apache OpenMeetings 6.0.0	7.5	More Details
CVE-2020-36277	Leptonica before 1.80.0 allows a denial of service (application crash) via an incorrect left shift in pixConvert2To8 in pixconv.c.	7.5	More Details
CVE-2021-22713	A CWE-119:Improper restriction of operations within the bounds of a memory buffer vulnerability exists in PowerLogic ION8650, ION8800, ION7650, ION7700/73xx, and ION83xx/84xx/85xx/8600 (see security notifcation for affected versions), which could cause the meter to reboot.	7.5	More Details
CVE-2021-27063	Windows DNS Server Denial of Service Vulnerability	7.5	More Details
CVE-2021-28374	The Debian courier-authlib package before 0.71.1-2 for Courier Authentication Library creates a /run/courier/authdaemon directory with weak permissions, allowing an attacker to read user information. This may include a cleartext password in some configurations. In general, it includes the user's existence, uid and gids, home and/or Maildir directory, quota, and some type of password information (such as a hash).	7.5	More Details
CVE-2021-3127	NATS Server 2.x before 2.2.0 and JWT library before 2.0.1 have Incorrect Access Control because Import Token bindings are mishandled.	7.5	More Details
CVE-2021-28373	The auth_internal plugin in Tiny Tiny RSS (aka tt-rss) before 2021-03-12 allows an attacker to log in via the OTP code without a valid password. NOTE: this issue only affected the git master branch for a short time. However, all end users are explicitly directed to use the git master branch in production. Semantic version numbers such as 21.03 appear to exist, but are automatically generated from the year and month. They are not releases.	7.5	More Details
CVE-2020-36280	Leptonica before 1.80.0 allows a heap-based buffer over-read in pixReadFromTiffStream, related to tiffio.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28361	An issue was discovered in Storage Performance Development Kit (SPDK) before 20.01.01. If a PDU is sent to the iSCSI target with a zero length (but data is expected), the iSCSI target can crash with a NULL pointer dereference.	7.5	More Details
CVE-2020-36281	Leptonica before 1.80.0 allows a heap-based buffer over-read in pixFewColorsOctcubeQuantMixed in colorquant1.c.	7.5	More Details
CVE-2021-26923	An issue was discovered in Argo CD before 1.8.4. Accessing the endpoint /api/version leaks internal information for the system, and this endpoint is not protected with authentication.	7.5	More Details
CVE-2021-28092	The is-svg package 2.1.0 through 4.2.1 for Node.js uses a regular expression that is vulnerable to Regular Expression Denial of Service (ReDoS). If an attacker provides a malicious string, is-svg will get stuck processing the input for a very long time.	7.5	More Details
CVE-2021-28295	Online Ordering System 1.0 is vulnerable to unauthenticated SQL injection through /onlineordering/GPST/admin/design.php, which may lead to database information disclosure.	7.5	More Details
CVE-2021-24029	A packet of death scenario is possible in mvfst via a specially crafted message during a QUIC session, which causes a crash via a failed assertion. Per QUIC specification, this particular message should be treated as a connection error. This issue affects mvfst versions prior to commit a67083ff4b8dcbb7ee2839da6338032030d712b0 and proxygen versions prior to v2021.03.15.00.	7.5	More Details
CVE-2021-27290	ssri 5.2.2-8.0.0, fixed in 8.0.1, processes SRIs using a regular expression which is vulnerable to a denial of service. Malicious SRIs could take an extremely long time to process, leading to denial of service. This issue only affects consumers using the strict option.	7.5	More Details
CVE-2020-36278	Leptonica before 1.80.0 allows a heap-based buffer over-read in findNextBorderPixel in ccbord.c.	7.5	More Details
CVE-2020-36279	Leptonica before 1.80.0 allows a heap-based buffer over-read in rasteropGeneralLow, related to adaptmap_reg.c and adaptmap.c.	7.5	More Details
CVE-2020-4831	IBM DataPower Gateway 10.0.0.0 through 10.0.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 189965.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28302	A stack overflow in pupnp before version 1.14.5 can cause the denial of service through the Parser_parseDocument() function. ixmlNode_free() will release a child node recursively, which will consume stack space and lead to a crash.	7.5	More Details
CVE-2021-28307	An issue was discovered in the fltk crate before 0.15.3 for Rust. There is a NULL pointer dereference during attempted use of a non-raster image for a window icon.	7.5	More Details
CVE-2021-28306	An issue was discovered in the fltk crate before 0.15.3 for Rust. There is a NULL pointer dereference during attempted use of a multi label type if the image is nonexistent.	7.5	More Details
CVE-2021-25676	A vulnerability has been identified in RUGGEDCOM RM1224 (V6.3), SCALANCE M-800 (V6.3), SCALANCE S615 (V6.3), SCALANCE SC-600 (All Versions >= V2.1 and < V2.1.3). Multiple failed SSH authentication attempts could trigger a temporary Denial-of-Service under certain conditions. When triggered, the device will reboot automatically.	7.5	More Details
CVE-2020-29238	An integer buffer overflow in the Nginx webserver of ExpressVPN Router version 1 allows remote attackers to obtain sensitive information when the server running as reverse proxy via specially crafted request.	7.5	More Details
CVE-2020-1919	Incorrect bounds calculations in substr_compare could lead to an out-of-bounds read when the second string argument passed in is longer than the first. This issue affects HHVM versions prior to 4.56.3, all versions between 4.57.0 and 4.80.1, all versions between 4.81.0 and 4.93.1, and versions 4.94.0, 4.95.0, 4.96.0, 4.97.0, 4.98.0.	7.5	More Details
CVE-2020-1918	In-memory file operations (ie: using fopen on a data URI) did not properly restrict negative seeking, allowing for the reading of memory prior to the in-memory buffer. This issue affects HHVM versions prior to 4.56.3, all versions between 4.57.0 and 4.80.1, all versions between 4.81.0 and 4.93.1, and versions 4.94.0, 4.95.0, 4.96.0, 4.97.0, 4.98.0.	7.5	More Details
CVE-2020-5024	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated attacker to cause a denial of service due a hang in the SSL handshake response. IBM X-Force ID: 193660.	7.5	More Details
CVE-2020-1898	The fb_unserialize function did not impose a depth limit for nested deserialization. That meant a maliciously constructed string could cause deserialization to recurse, leading to stack exhaustion. This issue affected HHVM prior to v4.32.3, between versions 4.33.0 and 4.56.0, 4.57.0, 4.58.0, 4.58.1, 4.59.0, 4.60.0, 4.61.0, 4.62.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27632	In SIMATIC MV400 family versions prior to v7.0.6, the ISN generator is initialized with a constant value and has constant increments. An attacker could predict and hijack TCP sessions.	7.5	More Details
CVE-2021-27918	encoding/xml in Go before 1.15.9 and 1.16.x before 1.16.1 has an infinite loop if a custom TokenReader (for xml.NewTokenDecoder) returns EOF in the middle of an element. This can occur in the Decode, DecodeElement, or Skip method.	7.5	More Details
CVE-2020-19419	Incorrect Access Control in Emerson Smart Wireless Gateway 1420 4.6.59 allows remote attackers to obtain sensitive device information from the administrator console without authentication.	7.5	More Details
CVE-2020-1899	The unserialize() function supported a type code, "S", which was meant to be supported only for APC serialization. This type code allowed arbitrary memory addresses to be accessed as if they were static StringData objects. This issue affected HHVM prior to v4.32.3, between versions 4.33.0 and 4.56.0, 4.57.0, 4.58.0, 4.58.1, 4.59.0, 4.60.0, 4.61.0, 4.62.0.	7.5	More Details
CVE-2021-20670	Improper access control vulnerability in GROWI versions v4.2.2 and earlier allows a remote unauthenticated attacker to read the user's personal information and/or server's internal information via unspecified vectors.	7.5	More Details
CVE-2020-1921	In the crypt function, we attempt to null terminate a buffer using the size of the input salt without validating that the offset is within the buffer. This issue affects HHVM versions prior to 4.56.3, all versions between 4.57.0 and 4.80.1, all versions between 4.81.0 and 4.93.1, and versions 4.94.0, 4.95.0, 4.96.0, 4.97.0, 4.98.0.	7.5	More Details
CVE-2021-26879	Windows Network Address Translation (NAT) Denial of Service Vulnerability	7.5	More Details
CVE-2021-26881	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	7.5	More Details
CVE-2021-20218	A flaw was found in the fabric8 kubernetes-client in version 4.2.0 and after. This flaw allows a malicious pod/container to cause applications using the fabric8 kubernetes-client `copy` command to extract files outside the working path. The highest threat from this vulnerability is to integrity and system availability. This has been fixed in kubernetes-client-4.13.2 kubernetes-client-5.0.2 kubernetes-client-4.11.2 kubernetes-client-4.7.2	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27070	Windows 10 Update Assistant Elevation of Privilege Vulnerability	7.3	More Details
CVE-2020-4184	IBM Security Guardium 11.2 performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses. IBM X-Force ID: 174802..	7.3	More Details
CVE-2020-35227	A buffer overflow vulnerability in the access control section on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices (in the administration web panel) allows an attacker to inject IP addresses into the whitelist via the checkedList parameter to the delete command.	7.2	More Details
CVE-2021-27947	SQL Injection vulnerability in MyBB before 1.8.26 via the Copy Forum feature in Forum Management. (issue 2 of 3).	7.2	More Details
CVE-2020-14987	An issue was discovered in Bloomreach Experience Manager (brXM) 4.1.0 through 14.2.2. It allows remote attackers to execute arbitrary code because there is a mishandling of the capability for administrators to write and run Groovy scripts within the updater editor. An attacker must use an AST transforming annotation such as @Grab.	7.2	More Details
CVE-2021-27948	SQL Injection vulnerability in MyBB before 1.8.26 via User Groups. (issue 3 of 3).	7.2	More Details
CVE-2021-20671	Invalid file validation on the upload feature in GROWI versions v4.2.2 allows a remote attacker with administrative privilege to overwrite the files on the server, which may lead to arbitrary code execution.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21381	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In Flatpack since version 0.9.4 and before version 1.10.2 has a vulnerability in the "file forwarding" feature which can be used by an attacker to gain access to files that would not ordinarily be allowed by the app's permissions. By putting the special tokens `@@` and/or `@@u` in the Exec field of a Flatpak app's .desktop file, a malicious app publisher can trick flatpak into behaving as though the user had chosen to open a target file with their Flatpak app, which automatically makes that file available to the Flatpak app. This is fixed in version 1.10.2. A minimal solution is the first commit "`Disallow @@ and @@U usage in desktop files`". The follow-up commits "`dir: Reserve the whole @@ prefix`" and "`dir: Refuse to export .desktop files with suspicious uses of @@ tokens`" are recommended, but not strictly required. As a workaround, avoid installing Flatpak apps from untrusted sources, or check the contents of the exported `.desktop` files in `exports/share/applications/*.desktop` (typically `~/.local/share/flatpak/exports/share/applications/*.desktop` and `/var/lib/flatpak/exports/share/applications/*.desktop`) to make sure that literal filenames do not follow `@@` or `@@u`.	7.1	More Details
CVE-2021-1729	Windows Update Stack Setup Elevation of Privilege Vulnerability	7.1	More Details
CVE-2020-35226	NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices allow unauthenticated users to modify the switch DHCP configuration by sending the corresponding write request command.	7.1	More Details
CVE-2021-21072	Adobe Animate version 21.0.3 (and earlier) is affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.1	More Details
CVE-2021-26866	Windows Update Service Elevation of Privilege Vulnerability	7.1	More Details
CVE-2021-24095	DirectX Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-26862	Windows Installer Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26863	Windows Win32k Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-26873	Windows User Profile Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-27893	SSH Tectia Client and Server before 6.4.19 on Windows allow local privilege escalation in nonstandard conditions. ConnectSecure on Windows is affected.	7.0	More Details
CVE-2021-27055	Microsoft Visio Security Feature Bypass Vulnerability	7.0	More Details
CVE-2020-35225	The NSDP protocol implementation on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices was not properly validating the length of string parameters sent in write requests, potentially allowing denial of service attacks.	6.8	More Details
CVE-2021-27208	When booting a Zync-7000 SOC device from nand flash memory, the nand driver in the ROM does not validate the inputs when reading in any parameters in the nand's parameter page. IF a field read in from the parameter page is too large, this causes a buffer overflow that could lead to arbitrary code execution. Physical access and modification of the board assembly on which the Zynq-7000 SoC device mounted is needed to replace the original NAND flash memory with a NAND flash emulation device for this attack to be successful.	6.8	More Details
CVE-2020-35230	Multiple integer overflow parameters were found in the web administration panel on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices. Most of the integer parameters sent through the web server can be abused to cause a denial of service attack.	6.8	More Details
CVE-2021-21265	October is a free, open-source, self-hosted CMS platform based on the Laravel PHP Framework. In October before version 1.1.2, when running on poorly configured servers (i.e. the server routes any request, regardless of the HOST header to an October CMS instance) the potential exists for Host Header Poisoning attacks to succeed. This has been addressed in version 1.1.2 by adding a feature to allow a set of trusted hosts to be specified in the application. As a workaround one may set the configuration setting cms.linkPolicy to force.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15260	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In version 2.10 and earlier, PJSIP transport can be reused if they have the same IP address + port + protocol. However, this is insufficient for secure transport since it lacks remote hostname authentication. Suppose we have created a TLS connection to `sip.foo.com`, which has an IP address `100.1.1.1`. If we want to create a TLS connection to another hostname, say `sip.bar.com`, which has the same IP address, then it will reuse that existing connection, even though `100.1.1.1` does not have certificate to authenticate as `sip.bar.com`. The vulnerability allows for an insecure interaction without user awareness. It affects users who need access to connections to different destinations that translate to the same address, and allows man-in-the-middle attack if attacker can route a connection to another destination such as in the case of DNS spoofing.	6.8	More Details
CVE-2021-27075	Azure Virtual Machine Information Disclosure Vulnerability	6.8	More Details
CVE-2021-21368	msgpack5 is a msgpack v5 implementation for node.js and the browser. In msgpack5 before versions 3.6.1, 4.5.1, and 5.2.1 there is a "Prototype Poisoning" vulnerability. When msgpack5 decodes a map containing a key "__proto__", it assigns the decoded value to __proto__. Object.prototype.__proto__ is an accessor property for the receiver's prototype. If the value corresponding to the key __proto__ decodes to an object or null, msgpack5 sets the decoded object's prototype to that value. An attacker who can submit crafted MessagePack data to a service can use this to produce values that appear to be of other types; may have unexpected prototype properties and methods (for example length, numeric properties, and push et al if __proto__'s value decodes to an Array); and/or may throw unexpected exceptions when used (for example if the __proto__ value decodes to a Map or Date). Other unexpected behavior might be produced for other types. There is no effect on the global prototype. This "prototype poisoning" is sort of a very limited inversion of a prototype pollution attack. Only the decoded value's prototype is affected, and it can only be set to msgpack5 values (though if the victim makes use of custom codecs, anything could be a msgpack5 value). We have not found a way to escalate this to true prototype pollution (absent other bugs in the consumer's code). This has been fixed in msgpack5 version 3.6.1, 4.5.1, and 5.2.1. See the referenced GitHub Security Advisory for an example and more details.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0371	In nci_proc_rf_management_ntf of nci_hrcv.cc, there is a possible out of bounds read 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: AndroidVersions: Android-11Android ID: A-164440989	6.7	More Details
CVE-2021-0456	In the Citadel chip firmware, 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: AndroidVersions: Android kernelAndroid ID: A-174769927	6.7	More Details
CVE-2021-0455	In the Citadel chip firmware, 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: AndroidVersions: Android kernelAndroid ID: A-175116439	6.7	More Details
CVE-2021-0457	In the FingerTipS touch screen driver, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-157155375	6.7	More Details
CVE-2021-0461	In iaxxx_core_sensor_change_state of iaxxx-module.c, 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: AndroidVersions: Android kernelAndroid ID: A-175124074	6.7	More Details
CVE-2021-0462	In the NXP NFC firmware, there is a possible insecure firmware update due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-168799695	6.7	More Details
CVE-2021-23879	Unquoted service path vulnerability in McAfee Endpoint Product Removal (EPR) Tool prior to 21.2 allows local administrators to execute arbitrary code, with higher-level privileges, via execution from a compromised folder. The tool did not enforce and protect the execution path. Local admin privileges are required to place the files in the required location.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0370	In Write of NxpMfcReader.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169259605	6.7	More Details
CVE-2021-0454	In the Citadel chip firmware, 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: AndroidVersions: Android kernelAndroid ID: A-175117047	6.7	More Details
CVE-2020-35224	A buffer overflow vulnerability in the NSDP protocol authentication method on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices allows remote unauthenticated attackers to force a device reboot.	6.5	More Details
CVE-2021-20205	Libjpeg-turbo versions 2.0.91 and 2.0.90 is vulnerable to a denial of service vulnerability caused by a divide by zero when processing a crafted GIF image.	6.5	More Details
CVE-2021-21078	Adobe Creative Cloud Desktop Application version 5.3 (and earlier) is affected by an Unquoted Service Path vulnerability in CCXProcess that could allow an attacker to achieve arbitrary code execution in the process of the current user. Exploitation of this issue requires user interaction	6.5	More Details
CVE-2021-28363	The urllib3 library 1.26.x before 1.26.4 for Python omits SSL certificate validation in some cases involving HTTPS to HTTPS proxies. The initial connection to the HTTPS proxy (if an SSLContext isn't given via proxy_config) doesn't verify the hostname of the certificate. This means certificates for different servers that still validate properly with the default urllib3 SSLContext will be silently accepted.	6.5	More Details
CVE-2021-0368	In oggpack_look of bitwise.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169829774	6.5	More Details
CVE-2020-5016	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories on the system. When application security is disabled and JAX-RPC applications are present, an attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary xml files on the system. This does not occur if Application security is enabled. IBM X-Force ID: 193556.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0378	In getNbits of pvmp3_getbits.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154076193	6.5	More Details
CVE-2020-14989	An issue was discovered in Bloomreach Experience Manager (brXM) 4.1.0 through 14.2.2. It allows CSRF if the attacker uses GET where POST was intended.	6.5	More Details
CVE-2021-21375	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In PJSIP version 2.10 and earlier, after an initial INVITE has been sent, when two 183 responses are received, with the first one causing negotiation failure, a crash will occur. This results in a denial of service.	6.5	More Details
CVE-2020-35233	The TFTP server fails to handle multiple connections on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices, and allows external attackers to force device reboots by sending concurrent connections, aka a denial of service attack.	6.5	More Details
CVE-2021-3167	In Cloudera Data Engineering (CDE) 1.3.0, JWT authentication tokens are exposed to administrators in virtual cluster server logs.	6.5	More Details
CVE-2021-0379	In getUpTo17bits of pvmp3_getbits.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154075955	6.5	More Details
CVE-2021-0387	In FindQuotaDeviceForUuid of QuotaUtils.cpp, there is a possible use-after-free 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: AndroidVersions: Android-11Android ID: A-169421939	6.4	More Details
CVE-2021-20261	A race condition was found in the Linux kernels implementation of the floppy disk drive controller driver software. The impact of this issue is lessened by the fact that the default permissions on the floppy device (/dev/fd0) are restricted to root. If the permissions on the device have changed the impact changes greatly. In the default configuration root (or equivalent) permissions are required to attack this flaw.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3418	If certificates that signed grub are installed into db, grub can be booted directly. It will then boot any kernel without signature validation. The booted kernel will think it was booted in secureboot mode and will implement lockdown, yet it could have been tampered. This flaw is a reintroduction of CVE-2020-15705 and only affects grub2 versions prior to 2.06 and upstream and distributions using the shim_lock mechanism.	6.4	More Details
CVE-2021-22191	Improper URL handling in Wireshark 3.4.0 to 3.4.3 and 3.2.0 to 3.2.11 could allow remote code execution via via packet injection or crafted capture file.	6.3	More Details
CVE-2021-21334	In containerd (an industry-standard container runtime) before versions 1.3.10 and 1.4.4, containers launched through containerd's CRI implementation (through Kubernetes, crictl, or any other pod/container client that uses the containerd CRI service) that share the same image may receive incorrect environment variables, including values that are defined for other containers. If the affected containers have different security contexts, this may allow sensitive information to be unintentionally shared. If you are not using containerd's CRI implementation (through one of the mechanisms described above), you are not vulnerable to this issue. If you are not launching multiple containers or Kubernetes pods from the same image which have different environment variables, you are not vulnerable to this issue. If you are not launching multiple containers or Kubernetes pods from the same image in rapid succession, you have reduced likelihood of being vulnerable to this issue This vulnerability has been fixed in containerd 1.3.10 and containerd 1.4.4. Users should update to these versions.	6.3	More Details
CVE-2021-26892	Windows Extensible Firmware Interface Security Feature Bypass Vulnerability	6.2	More Details
CVE-2021-27074	Azure Sphere Unsigned Code Execution Vulnerability	6.2	More Details
CVE-2021-27938	A vulnerability has been identified in the Silverstripe CMS 3 and 4 version of the symbiote/silverstripe-queuedjobs module. A Cross Site Scripting vulnerability allows an attacker to inject an arbitrary payload in the CreateQueuedJobTask dev task via a specially crafted URL.	6.1	More Details
CVE-2021-26924	An issue was discovered in Argo CD before 1.8.4. Browser XSS protection is not activated due to the missing XSS protection header.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3150	A cross-site scripting (XSS) vulnerability on the Delete Personal Data page in Cryptshare Server before 4.8.0 allows an attacker to inject arbitrary web script or HTML via the user name. The issue is fixed with the version 4.8.1	6.1	More Details
CVE-2021-28162	In Eclipse Theia versions up to and including 0.16.0, in the notification messages there is no HTML escaping, so Javascript code can run.	6.1	More Details
CVE-2021-28161	In Eclipse Theia versions up to and including 1.8.0, in the debug console there is no HTML escaping, so arbitrary Javascript code can be injected.	6.1	More Details
CVE-2021-26886	User Profile Service Denial of Service Vulnerability	6.1	More Details
CVE-2021-20672	Reflected cross-site scripting vulnerability due to insufficient verification of URL query parameters in GROWI (v4.2 Series) versions from v4.2.0 to v4.2.7 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-21080	Adobe Connect version 11.0.7 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this vulnerability to inject malicious JavaScript content that may be executed within the context of the victim's browser when they browse to the page containing the vulnerable field.	6.1	More Details
CVE-2021-21079	Adobe Connect version 11.0.7 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this vulnerability to inject malicious JavaScript content that may be executed within the context of the victim's browser when they browse to the page containing the vulnerable field.	6.1	More Details
CVE-2021-21491	SAP Netweaver Application Server Java (Applications based on WebDynpro Java) versions 7.00, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allow an attacker to redirect users to a malicious site due to Reverse Tabnabbing vulnerabilities.	6.1	More Details
CVE-2021-28007	Web Based Quiz System 1.0 is affected by cross-site scripting (XSS) in register.php through the name parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21068	Adobe Creative Cloud Desktop Application version 5.3 (and earlier) is affected by a file handling vulnerability that could allow an attacker to cause arbitrary file overwriting. Exploitation of this issue requires physical access and user interaction.	6.1	More Details
CVE-2021-27889	Cross-site Scripting (XSS) vulnerability in MyBB before 1.8.26 via Nested Auto URL when parsing messages.	6.1	More Details
CVE-2021-21367	Switchboard Bluetooth Plug for elementary OS from version 2.3.0 and before version version 2.3.5 has an incorrect authorization vulnerability. When the Bluetooth plug is running (in discoverable mode), Bluetooth service requests and pairing requests are automatically accepted, allowing physically proximate attackers to pair with a device running an affected version of switchboard-plug-bluetooth without the active consent of the user. By default, elementary OS doesn't expose any services via Bluetooth that allow information to be extracted by paired Bluetooth devices. However, if such services (i.e. contact list sharing software) have been installed, it's possible that attackers have been able to extract data from such services without authorization. If no such services have been installed, attackers are only able to pair with a device running an affected version without authorization and then play audio out of the device or possibly present a HID device (keyboard, mouse, etc...) to control the device. As such, users should check the list of trusted/paired devices and remove any that are not 100% confirmed to be genuine. This is fixed in version 2.3.5. To reduce the likelihood of this vulnerability on an unpatched version, only open the Bluetooth plug for short intervals when absolutely necessary and preferably not in crowded public areas. To mitigate the risk entirely with unpatched versions, do not open the Bluetooth plug within switchboard at all, and use a different method for pairing devices if necessary (e.g. `bluetoothctl` CLI).	6.1	More Details
CVE-2021-27695	Multiple stored cross-site scripting (XSS) vulnerabilities in openMAINT 2.1-3.3-b allow remote attackers to inject arbitrary web script or HTML via any "Add" sections, such as Add Card Building & Floor, or others in the Name and Code Parameters.	6.1	More Details
CVE-2021-27949	Cross-site Scripting vulnerability in MyBB before 1.8.26 via Custom moderator tools.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13959	The default error page for VelocityView in Apache Velocity Tools prior to 3.1 reflects back the vm file that was entered as part of the URL. An attacker can set an XSS payload file as this vm file in the URL which results in this payload being executed. XSS vulnerabilities allow attackers to execute arbitrary JavaScript in the context of the attacked website and the attacked user. This can be abused to steal session cookies, perform requests in the name of the victim or for phishing attacks.	6.1	More Details
CVE-2020-1926	Apache Hive cookie signature verification used a non constant time comparison which is known to be vulnerable to timing attacks. This could allow recovery of another users cookie signature. The issue was addressed in Apache Hive 2.3.8	5.9	More Details
CVE-2021-23356	This affects all versions of package kill-process-by-name. If (attacker-controlled) user input is given, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization in the index.js file.	5.6	More Details
CVE-2021-23355	This affects all versions of package ps-kill. If (attacker-controlled) user input is given to the kill function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization in the index.js file. PoC (provided by reporter): var ps_kill = require('ps-kill'); ps_kill.kill('$(touch success)',function(){});	5.6	More Details
CVE-2021-0375	In onPackageModified of VoiceInteractionManagerService.java, there is a possible change of default applications due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-167261484	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25236	A vulnerability has been identified in LOGO! 12/24RCE (6ED1052-1MD08-0BA1) (All versions), LOGO! 12/24RCEo (6ED1052-2MD08-0BA1) (All versions), LOGO! 230RCE (6ED1052-1FB08-0BA1) (All versions), LOGO! 230RCEo (6ED1052-2FB08-0BA1) (All versions), LOGO! 24CE (6ED1052-1CC08-0BA1) (All versions), LOGO! 24CEo (6ED1052-2CC08-0BA1) (All versions), LOGO! 24RCE (6ED1052-1HB08-0BA1) (All versions), LOGO! 24RCEo (6ED1052-2HB08-0BA1) (All versions), SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA1) (All versions), SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA1) (All versions), SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA1) (All versions), SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA1) (All versions), SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA1) (All versions), SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA1) (All versions), SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA1) (All versions), SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA1) (All versions). The control logic (CL) the LOGO! 8 executes could be manipulated in a way that could cause the device executing the CL to improperly handle the manipulation and crash. After successful execution of the attack, the device needs to be manually reset.	5.5	More Details
CVE-2020-29556	The Backup functionality in Grav CMS through 1.7.0-rc.17 allows an authenticated attacker to read arbitrary local files on the underlying server by exploiting a path-traversal technique. (This vulnerability can also be exploited by an unauthenticated attacker due to a lack of CSRF protection.)	5.5	More Details
CVE-2021-27919	archive/zip in Go 1.16.x before 1.16.1 allows attackers to cause a denial of service (panic) upon attempted use of the Reader.Open API for a ZIP archive in which ../ occurs at the beginning of any filename.	5.5	More Details
CVE-2020-28387	A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP3). When opening a specially crafted SEECTCXML file, the application could disclose arbitrary files to remote attackers. This is because of the passing of specially crafted content to the underlying XML parser without taking proper restrictions such as prohibiting an external dtd. (ZDI-CAN-11923)	5.5	More Details
CVE-2021-25675	A vulnerability has been identified in SIMATIC S7-PLCSIM V5.4 (All versions). An attacker with local access to the system could cause a Denial-of-Service condition in the application when it is used to open a specially crafted file. As a consequence, a divide by zero operation could occur and cause the application to terminate unexpectedly and must be restarted to restore the service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4717	A vulnerability exists in IBM SPSS Modeler Subscription Installer that allows a user with create symbolic link permission to write arbitrary file in another protected path during product installation. IBM X-Force ID: 187727.	5.5	More Details
CVE-2021-20265	A flaw was found in the way memory resources were freed in the unix_stream_recvmsg function in the Linux kernel when a signal was pending. This flaw allows an unprivileged local user to crash the system by exhausting available memory. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2021-25673	A vulnerability has been identified in SIMATIC S7-PLCSIM V5.4 (All versions). An attacker with local access to the system could cause a Denial-of-Service condition in the application when it is used to open a specially crafted file. As a consequence, the application could enter an infinite loop, become unresponsive and must be restarted to restore the service.	5.5	More Details
CVE-2021-25674	A vulnerability has been identified in SIMATIC S7-PLCSIM V5.4 (All versions). An attacker with local access to the system could cause a Denial-of-Service condition in the application when it is used to open a specially crafted file. As a consequence, a NULL pointer deference condition could cause the application to terminate unexpectedly and must be restarted to restore the service.	5.5	More Details
CVE-2021-0377	In DeltaPerformer::Write of delta_performer.cc, there is a possible use of untrusted input due to improper input validation. This could lead to a local bypass of defense in depth protections with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-160800689	5.5	More Details
CVE-2021-0394	In android_os_Parcel_readString8 of android_os_Parcel.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-172655291	5.5	More Details
CVE-2020-4851	IBM Spectrum Scale 5.0.0 through 5.0.5.5 and 5.1.0 through 5.1.0.2 could allow a local user to poison log files which could impact support and development efforts. IBM X-Force ID: 190450.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0381	In updateNotifications of DeviceStorageMonitorService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153466381	5.5	More Details
CVE-2021-24107	Windows Event Tracing Information Disclosure Vulnerability	5.5	More Details
CVE-2021-26869	Windows ActiveX Installer Service Information Disclosure Vulnerability	5.5	More Details
CVE-2021-0463	In convertToHidl of convert.cpp, there is a possible out of bounds read due to uninitialized data from ReturnFrameworkMessage. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-154867068	5.5	More Details
CVE-2021-0382	In checkSlicePermission of SliceManagerService.java, there is a possible resource exposure due to an incorrect permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-140727941	5.5	More Details
CVE-2021-26884	Windows Media Photo Codec Information Disclosure Vulnerability	5.5	More Details
CVE-2020-4891	IBM Spectrum Scale 5.0.0 through 5.0.5.5 and 5.1.0 through 5.1.0.2 uses an inadequate account lockout setting that could allow a local user er to brute force Rest API account credentials. IBM X-Force ID: 190974.	5.5	More Details
CVE-2021-27677	Cross-site scripting (XSS) vulnerability in Galleries in Batflat CMS 1.3.6 allows remote attackers to inject arbitrary web script or HTML via the field name.	5.4	More Details
CVE-2021-20280	Text-based feedback answers required additional sanitizing to prevent stored XSS and blind SSRF risks in moodle before 3.10.2, 3.9.5, 3.8.8, 3.5.17.	5.4	More Details
CVE-2021-20667	Stored cross-site scripting vulnerability due to inadequate CSP (Content Security Policy) configuration in GROWI versions v4.2.2 and earlier allows remote authenticated attackers to inject an arbitrary script via a specially crafted content.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28380	The aimeos (aka Aimeos shop and e-commerce framework) extension before 19.10.12 and 20.x before 20.10.5 for TYPO3 allows XSS via a backend user account.	5.4	More Details
CVE-2021-26776	CSZ CMS 1.2.9 is affected by a cross-site scripting (XSS) vulnerability in multiple pages through the field name.	5.4	More Details
CVE-2020-35752	Baby Care System 1.0 is affected by a cross-site scripting (XSS) vulnerability in the Edit Page tab through the Post title parameter.	5.4	More Details
CVE-2021-27678	Cross-site scripting (XSS) vulnerability in Snippets in Batflat CMS 1.3.6 allows remote attackers to inject arbitrary web script or HTML via the field name.	5.4	More Details
CVE-2021-27679	Cross-site scripting (XSS) vulnerability in Navigation in Batflat CMS 1.3.6 allows remote attackers to inject arbitrary web script or HTML via the field name.	5.4	More Details
CVE-2021-28088	Cross-site scripting (XSS) in modules/content/admin/content.php in ImpressCMS profile 1.4.2 allows remote attackers to inject arbitrary web script or HTML parameters through the "Display Name" field.	5.4	More Details
CVE-2021-20279	The ID number user profile field required additional sanitizing to prevent a stored XSS risk in moodle before 3.10.2, 3.9.5, 3.8.8, 3.5.17.	5.4	More Details
CVE-2021-3224	A stored cross-site scripting (XSS) vulnerability in cszcms 1.2.9 exists in /admin/pages/new via the content parameter.	5.4	More Details
CVE-2020-14988	An issue was discovered in Bloomreach Experience Manager (brXM) 4.1.0 through 14.2.2. It allows XSS in the login page via the loginmessage parameter, the text editor via the src attribute of HTML elements, the translations menu via the foldername parameter, the author page via the link URL, or the upload image functionality via an SVG document containing JavaScript.	5.4	More Details
CVE-2020-23721	An issue was discovered in FUEL CMS V1.4.7. An attacker can use a XSS payload and bypass a filter via /fuelCM/fuel/pages/edit/1?lang=english.	5.4	More Details
CVE-2021-20336	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-3897	It has been discovered in redhat-certification that any unauthorized user may download any file under /var/www/rhcert, provided they know its name. Red Hat Certification 6 and 7 is vulnerable to this issue.	5.3	More Details
CVE-2021-23354	The package printf before 0.6.1 are vulnerable to Regular Expression Denial of Service (ReDoS) via the regex string /\%(?:\(([\w_.]+)\)|([1-9]\d*)\$)?([0 +\-\]*)(*|\d+)?(\.)?(*|\d+)?[hlL]?([\%bscdeEfFgGioOuxX])/g in lib/printf.js. The vulnerable regular expression has cubic worst-case time complexity.	5.3	More Details
CVE-2021-21363	swagger-codegen is an open-source project which contains a template-driven engine to generate documentation, API clients and server stubs in different languages by parsing your OpenAPI / Swagger definition. In swagger-codegen before version 2.4.19, on Unix like systems, the system's temporary directory is shared between all users on that system. A collocated user can observe the process of creating a temporary sub directory in the shared temporary directory and race to complete the creation of the temporary subdirectory. This vulnerability is local privilege escalation because the contents of the `outputFolder` can be appended to by an attacker. As such, code written to this directory, when executed can be attacker controlled. For more details refer to the referenced GitHub Security Advisory. This vulnerability is fixed in version 2.4.19. Note this is a distinct vulnerability from CVE-2021-21364.	5.3	More Details
CVE-2021-21364	swagger-codegen is an open-source project which contains a template-driven engine to generate documentation, API clients and server stubs in different languages by parsing your OpenAPI / Swagger definition. In swagger-codegen before version 2.4.19, on Unix-Like systems, the system temporary directory is shared between all local users. When files/directories are created, the default `umask` settings for the process are respected. As a result, by default, most processes/apis will create files/directories with the permissions `-rw-r--r--` and `drwxr-xr-x` respectively, unless an API that explicitly sets safe file permissions is used. Because this vulnerability impacts generated code, the generated code will remain vulnerable until fixed manually! This vulnerability is fixed in version 2.4.19. Note this is a distinct vulnerability from CVE-2021-21363.	5.3	More Details
CVE-2021-28153	An issue was discovered in GNOME GLib before 2.66.8. When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.)	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27052	Microsoft SharePoint Server Information Disclosure Vulnerability	5.3	More Details
CVE-2021-20282	When creating a user account, it was possible to verify the account without having access to the verification email link/secret in moodle before 3.10.2, 3.9.5, 3.8.8, 3.5.17.	5.3	More Details
CVE-2021-20281	It was possible for some users without permission to view other users' full names to do so via the online users block in moodle before 3.10.2, 3.9.5, 3.8.8, 3.5.17.	5.3	More Details
CVE-2020-27278	In Hamilton Medical AG,T1-Ventillator versions 2.2.3 and prior, hard-coded credentials in the ventilator allow attackers with physical access to obtain admin privileges for the device’s configuration interface.	5.2	More Details
CVE-2021-3034	An information exposure through log file vulnerability exists in Cortex XSOAR software where the secrets configured for the SAML single sign-on (SSO) integration can be logged to the '/var/log/demisto/' server logs when testing the integration during setup. This logged information includes the private key and identity provider certificate used to configure the SAML SSO integration. This issue impacts: Cortex XSOAR 5.5.0 builds earlier than 98622; Cortex XSOAR 6.0.1 builds earlier than 830029; Cortex XSOAR 6.0.2 builds earlier than 98623; Cortex XSOAR 6.1.0 builds earlier than 848144.	5.1	More Details
CVE-2021-21371	Tenable for Jira Cloud is an open source project designed to pull Tenable.io vulnerability data, then generate Jira Tasks and sub-tasks based on the vulnerabilities' current state. It published in pypi as "tenable-jira-cloud". In tenable-jira-cloud before version 1.1.21, it is possible to run arbitrary commands through the yaml.load() method. This could allow an attacker with local access to the host to run arbitrary code by running the application with a specially crafted YAML configuration file. This is fixed in version 1.1.21 by using yaml.safe_load() instead of yaml.load().	5.0	More Details
CVE-2021-20018	A post-authenticated vulnerability in SonicWall SMA100 allows an attacker to export the configuration file to the specified email address. This vulnerability impacts SMA100 version 10.2.0.5 and earlier.	4.9	More Details
CVE-2021-20673	Stored cross-site scripting vulnerability in Admin Page of GROWI (v4.2 Series) versions from v4.2.0 to v4.2.7 allows remote authenticated attackers to inject an arbitrary script via unspecified vectors.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35228	A cross-site scripting (XSS) vulnerability in the administration web panel on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices allows remote attackers to inject arbitrary web script or HTML via the language parameter.	4.8	More Details
CVE-2021-20669	Path traversal vulnerability in GROWI versions v4.2.2 and earlier allows an attacker with administrator rights to read and/or delete an arbitrary path via a specially crafted URL.	4.7	More Details
CVE-2021-24104	Microsoft SharePoint Server Spoofing Vulnerability	4.6	More Details
CVE-2020-4890	IBM Spectrum Scale 5.0.0 through 5.0.5.5 and 5.1.0 through 5.1.0.2 could allow a local user with a valid role to the REST API to cause a denial of service due to weak or absense of rate limiting. IBM X-Force ID: 190973.	4.4	More Details
CVE-2020-4976	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to read and write specific files due to weak file permissions. IBM X-Force ID: 192469.	4.4	More Details
CVE-2021-0458	In the FingerTipS touch screen driver, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-157156744	4.4	More Details
CVE-2021-0453	In the Titan-M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117199	4.4	More Details
CVE-2021-0374	In BnAudioPolicyService::onTransact of IAudioPolicyService.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169572641	4.4	More Details
CVE-2021-0459	In fts_driver_test_write of fts_proc.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-157154534	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0460	In the FingerTipS touch screen driver, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-156739245	4.4	More Details
CVE-2021-0452	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117261	4.4	More Details
CVE-2021-0450	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117880	4.4	More Details
CVE-2021-0449	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117965	4.4	More Details
CVE-2021-0451	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117871	4.4	More Details
CVE-2020-27282	In Hamilton Medical AG,T1-Ventillator versions 2.2.3 and prior, an XML validation vulnerability in the ventilator allows privileged attackers with physical access to render the device persistently unusable by uploading specially crafted configuration files.	4.3	More Details
CVE-2021-20283	The web service responsible for fetching other users' enrolled courses did not validate that the requesting user had permission to view that information in each course in moodle before 3.10.2, 3.9.5, 3.8.8, 3.5.17.	4.3	More Details
CVE-2020-24982	An issue was discovered in Quadbase ExpressDashboard (EDAB) 7 Update 9. It allows CSRF. An attacker may be able to trick an authenticated user into changing the email address associated with their account.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27066	Windows Admin Center Security Feature Bypass Vulnerability	4.3	More Details
CVE-2020-27290	In Hamilton Medical AG,T1-Ventillator versions 2.2.3 and prior, an information disclosure vulnerability in the ventilator allows attackers with physical access to the configuration interface's logs to get valid checksums for tampered configuration files.	4.3	More Details
CVE-2021-21366	xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) DOMParser and XMLSerializer module. xmldom versions 0.4.0 and older do not correctly preserve system identifiers, FPIs or namespaces when repeatedly parsing and serializing maliciously crafted documents. This may lead to unexpected syntactic changes during XML processing in some downstream applications. This is fixed in version 0.5.0. As a workaround downstream applications can validate the input and reject the maliciously crafted documents.	4.3	More Details
CVE-2020-28705	FUEL CMS 1.4.13 contains a cross-site request forgery (CSRF) vulnerability that can delete a page via a post ID to /pages/delete/3.	4.3	More Details
CVE-2021-20440	IBM API Connect 10.0.0.0, and 2018.4.1.0 through 2018.4.1.13 does not restrict member registration to the intended recepient. An attacker who is a valid user in the user registry used by API Manager can use a stolen invitation link and register themselves as a member of an API provider organization. IBM X-Force ID: 196536.	4.3	More Details
CVE-2021-28543	Varnish varnish-modules before 0.17.1 allows remote attackers to cause a denial of service (daemon restart) in some configurations. This does not affect organizations that only install the Varnish Cache product; however, it is common to install both Varnish Cache and varnish-modules. Specifically, an assertion failure or NULL pointer dereference can be triggered in Varnish Cache through the varnish-modules header.append() and header.copy() functions. For some Varnish Configuration Language (VCL) files, this gives remote clients an opportunity to cause a Varnish Cache restart. A restart reduces overall availability and performance due to an increased number of cache misses, and may cause higher load on backend servers.	4.0	More Details
CVE-2021-28378	Gitea 1.12.x and 1.13.x before 1.13.4 allows XSS via certain issue data in some situations.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23357	All versions of package github.com/tyktechnologies/tyk/gateway are vulnerable to Directory Traversal via the handleAddOrUpdateApi function. This function is able to delete arbitrary JSON files on the disk where Tyk is running via the management API. The APIID is provided by the user and this value is then used to create a file on disk. If there is a file found with the same name then it will be deleted and then re-created with the contents of the API creation request.	3.3	More Details
CVE-2021-20286	A flaw was found in libnbd 1.7.3. An assertion failure in nbd_unlocked_opt_go in ilb/opt.c may lead to denial of service.	2.7	More Details
CVE-2021-20668	Path traversal vulnerability in GROWI versions v4.2.2 and earlier allows an attacker with administrator rights to read an arbitrary path via a specially crafted URL.	2.7	More Details
CVE-2021-21726	Some ZTE products have an input verification vulnerability in the diagnostic function interface. Due to insufficient verification of some parameters input by users, an attacker with high privileges can cause process exception by repeatedly inputting illegal parameters. This affects: <ZXONE 9700 , ZXONE 8700, ZXONE 19700><V1.40.021.021CP049, V1.0P02B219_@NCPM-RELEASE_2.40R1-20200914.set>	2.3	More Details
CVE-2021-22887	A vulnerability in the BIOS of Pulse Secure (PSA-Series Hardware) models PSA5000 and PSA7000 could allow an attacker to compromise BIOS firmware. This vulnerability can be exploited only as part of an attack chain. Before an attacker can compromise the BIOS, they must exploit the device.	2.3	More Details
CVE-2021-21071	Adobe Animate version 21.0.3 (and earlier) is affected by a Memory Corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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-2019-3903	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2019-3898	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2019-3853	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 Number	Description	Base Score	Reference
CVE-2021-21056	Adobe Framemaker version 2020.0.1 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve 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-2021-21069	Adobe Creative Cloud Desktop Application version 5.3 (and earlier) is affected by a local privilege escalation vulnerability that could allow an attacker to call functions against the installer to perform high privileged actions. Exploitation of this issue does not require user interaction.	N/A	More Details
CVE-2020-35232	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-35782. Reason: This candidate is a reservation duplicate of CVE-2020-35782. Notes: All CVE users should reference CVE-2020-35782 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-21073	Adobe Animate version 21.0.3 (and earlier) is affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information 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-2021-21074	Adobe Animate version 21.0.3 (and earlier) is affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information 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-2021-0384	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-2021-21076	Adobe Animate version 21.0.3 (and earlier) is affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information 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-2021-21077	Adobe Animate version 21.0.3 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve 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 Number	Description	Base Score	Reference
CVE-2020-35220	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-35801. Reason: This candidate is a reservation duplicate of CVE-2020-35801. Notes: All CVE users should reference CVE-2020-35801 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-35222	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-35783. Reason: This candidate is a reservation duplicate of CVE-2020-35783. Notes: All CVE users should reference CVE-2020-35783 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-21075	Adobe Animate version 21.0.3 (and earlier) is affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information 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