SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 08 September 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-2021-39199	remark-html is an open source nodejs library which compiles Markdown to HTML. In affected versions the documentation of remark-html has mentioned that it was safe by default. In practice the default was never safe and had to be opted into. That is, user input was not sanitized. This means arbitrary HTML can be passed through leading to potential XSS attacks. The problem has been patched in 13.0.2 and 14.0.1: `remark-html` is now safe by default, and the implementation matches the documentation. On older affected versions, pass `sanitize: true` if you cannot update.	10.0	More Details
CVE-2021-3757	immer is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	9.8	More Details
CVE-2021-38840	SQL Injection can occur in Simple Water Refilling Station Management System 1.0 via the water_refilling/classes/Login.php username parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40494	A Hardcoded JWT Secret Key in metadata.py in AdaptiveScale LXDUI through 2.1.3 allows attackers to gain admin access to the host system.	9.8	More Details
CVE-2019-10095	bash command injection vulnerability in Apache Zeppelin allows an attacker to inject system commands into Spark interpreter settings. This issue affects Apache Zeppelin Apache Zeppelin version 0.9.0 and prior versions.	9.8	More Details
CVE-2021-40353	A SQL injection vulnerability exists in version 8.0 of openSIS when MySQL or MariaDB is used as the application database. An attacker can then issue the SQL command through the index.php USERNAME parameter. NOTE: this issue may exist because of an incomplete fix for CVE-2020-6637.	9.8	More Details
CVE-2021-34746	A vulnerability in the TACACS+ authentication, authorization and accounting (AAA) feature of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an unauthenticated, remote attacker to bypass authentication and log in to an affected device as an administrator. This vulnerability is due to incomplete validation of user-supplied input that is passed to an authentication script. An attacker could exploit this vulnerability by injecting parameters into an authentication request. A successful exploit could allow the attacker to bypass authentication and log in as an administrator to the affected device.	9.8	More Details
CVE-2021-3766	objection.js is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	9.8	More Details
CVE-2021-40350	webctrl.cgi.elf on Christie Digital DWU850-GS V06.46 devices allows attackers to perform any desired action via a crafted query containing an unspecified Cookie header. Authentication bypass can be achieved by including an administrative cookie that the device does not validate.	9.8	More Details
CVE-2021-40531	Sketch before 75 allows library feeds to be used to bypass file quarantine. Files are automatically downloaded and opened, without the com.apple.quarantine extended attribute. This results in remote code execution, as demonstrated by CommandString in a terminal profile to Terminal.app.	9.8	More Details
CVE-2021-40532	Telegram Web K Alpha before 0.7.2 mishandles the characters in a document extension.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40540	ulfius_uri_logger in Ulfius HTTP Framework before 2.7.4 omits con_info initialization and a con_info->request NULL check for certain malformed HTTP requests.	9.8	More Details
CVE-2021-36163	In Apache Dubbo, users may choose to use the Hessian protocol. The Hessian protocol is implemented on top of HTTP and passes the body of a POST request directly to a HessianSkeleton: New HessianSkeleton are created without any configuration of the serialization factory and therefore without applying the dubbo properties for applying allowed or blocked type lists. In addition, the generic service is always exposed and therefore attackers do not need to figure out a valid service/method name pair. This is fixed in 2.7.13, 2.6.10.1	9.8	More Details
CVE-2021-34436	In Eclipse Theia 0.1.1 to 0.2.0, it is possible to exploit the default build to obtain remote code execution (and XXE) via the theia-xml-extension. This extension uses lsp4xml (recently renamed to LemMinX) in order to provide language support for XML. This is installed by default.	9.8	More Details
CVE-2021-37716	A remote buffer overflow vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	9.8	More Details
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus version 6113 and prior is vulnerable to REST API authentication bypass with resultant remote code execution.	9.8	More Details
CVE-2021-35946	A receiver of a federated share with access to the database with ownCloud version before 10.8 could update the permissions and therefore elevate their own permissions.	9.8	More Details
CVE-2021-39497	eyoucms 1.5.4 lacks sanitization of input data, allowing an attacker to inject a url to trigger blind SSRF via the saveRemote() function.	9.8	More Details
CVE-2021-39379	A SQL Injection vulnerability exists in openSIS 8.0 when MySQL (MariaDB) is being used as the application database. A malicious attacker can issue SQL commands to the MySQL (MariaDB) database through the ResetUserInfo.php password_stn_id parameter.	9.8	More Details
CVE-2021-39378	A SQL Injection vulnerability exists in openSIS 8.0 when MySQL (MariaDB) is being used as the application database. A malicious attacker can issue SQL commands to the MySQL (MariaDB) database through the NamesList.php str parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39377	A SQL Injection vulnerability exists in openSIS 8.0 when MySQL (MariaDB) is being used as the application database. A malicious attacker can issue SQL commands to the MySQL (MariaDB) database through the index.php username parameter.	9.8	More Details
CVE-2021-37415	Zoho ManageEngine ServiceDesk Plus before 11302 is vulnerable to authentication bypass that allows a few REST-API URLs without authentication.	9.8	More Details
CVE-2020-18048	An issue in craigms/main.php of CraigMS 1.0 allows attackers to execute arbitrary commands via a crafted input entered into the DB Name field.	9.8	More Details
CVE-2020-7819	A SQL-Injection vulnerability in the nTracker USB Enterprise(secure USB management solution) allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information.	9.3	More Details
CVE-2021-32802	Nextcloud server is an open source, self hosted personal cloud. Nextcloud supports rendering image previews for user provided file content. For some image types, the Nextcloud server was invoking a third-party library that wasn't suited for untrusted user-supplied content. There are several security concerns with passing user-generated content to this library, such as Server-Side-Request-Forgery, file disclosure or potentially executing code on the system. The risk depends on your system configuration and the installed library version. It is recommended that the Nextcloud Server is upgraded to 20.0.12, 21.0.4 or 22.1.0. These versions do not use this library anymore. As a workaround users may disable previews by setting `enable_previews` to `false` in `config.php`.	9.3	More Details
CVE-2021-22704	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Harmony/HMI Products Configured by Vijeo Designer (all versions prior to V6.2 SP11), Vijeo Designer Basic (all versions prior to V1.2), or EcoStruxure Machine Expert (all versions prior to V2.0) that could cause a Denial of Service or unauthorized access to system information when connecting to the Harmony HMI over FTP.	9.1	More Details
CVE-2021-39185	Http4s is a minimal, idiomatic Scala interface for HTTP services. In http4s versions 0.21.26 and prior, 0.22.0 through 0.22.2, 0.23.0, 0.23.1, and 1.0.0-M1 through 1.0.0-M24, the default CORS configuration is vulnerable to an origin reflection attack. The middleware is also susceptible to a Null Origin Attack. The problem is fixed in 0.21.27, 0.22.3, 0.23.2, and 1.0.0-M25. The original `CORS` implementation and `CORSConfig` are deprecated. See the GitHub GHSA for more information, including code examples and workarounds.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36042	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability in the API File Option Upload Extension. An attacker with Admin privileges can achieve unrestricted file upload which can result in remote code execution.	9.1	More Details
CVE-2021-36041	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges could upload a specially crafted file in the 'pub/media` directory could lead to remote code execution.	9.1	More Details
CVE-2021-36040	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges can upload a specially crafted file to bypass file extension restrictions and could lead to remote code execution.	9.1	More Details
CVE-2021-36035	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges could make a crafted request to the Adobe Stock API to achieve remote code execution.	9.1	More Details
CVE-2021-36034	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges can upload a specially crafted file to achieve remote code execution.	9.1	More Details
CVE-2021-36033	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability in the Widgets Module. An attacker with admin privileges can trigger a specially crafted script to achieve remote code execution.	9.1	More Details
CVE-2021-36029	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper improper authorization vulnerability. An attacker with admin privileges could leverage this vulnerability to achieve remote code execution.	9.1	More Details
CVE-2021-36028	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability when saving a configurable product. An attacker with admin privileges can trigger a specially crafted script to achieve remote code execution.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36025	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability while saving a customer's details with a specially crafted file. An authenticated attacker with admin privileges can leverage this vulnerability to achieve remote code execution.	9.1	More Details
CVE-2020-19751	An issue was discovered in gpac 0.8.0. The gf_odf_del_ipmp_tool function in odf_code.c has a heap-based buffer over-read.	9.1	More Details
CVE-2021-36024	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an Improper Neutralization of Special Elements Used In A Command via the Data collection endpoint. An attacker with admin privileges can upload a specially crafted file to achieve remote code execution.	9.1	More Details
CVE-2021-36022	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability in the Widgets Update Layout. An attacker with admin privileges can trigger a specially crafted script to achieve remote code execution.	9.1	More Details
CVE-2020-20495	bludit v3.13.0 contains an arbitrary file deletion vulnerability in the backup plugin via the `deleteBackup' parameter.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-35218	Deserialization of Untrusted Data in the Web Console Chart Endpoint can lead to remote code execution. An unauthorized attacker who has network access to the Orion Patch Manager Web Console could potentially exploit this and compromise the server	8.9	More Details
CVE-2021-35216	Insecure Deserialization of untrusted data remote code execution vulnerability was discovered in Patch Manager Orion Platform Integration module. An Authenticated Attacker with network access via HTTP can compromise this vulnerability can result in Remote Code Execution.	8.9	More Details
CVE-2021-35215	Insecure deserialization leading to Remote Code Execution was detected in the Orion Platform version 2020.2.5. Authentication is required to exploit this vulnerability.	8.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30618	Chromium: CVE-2021-30618 Inappropriate implementation in DevTools	8.8	More Details
CVE-2021-24391	An editid GET parameter of the Cashtomer WordPress plugin through 1.0.0 is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	8.8	More Details
CVE-2021-38617	In Eigen NLP 3.10.1, a lack of access control on the /auth/v1/user/ user creation endpoint allows a standard user to create a super user account with a defined password. This directly leads to privilege escalation.	8.8	More Details
CVE-2021-30624	Chromium: CVE-2021-30624 Use after free in Autofill	8.8	More Details
CVE-2021-38706	messages_load.php in ClinicCases 7.3.3 suffers from a blind SQL injection vulnerability, which allows low-privileged attackers to execute arbitrary SQL commands through a vulnerable parameter.	8.8	More Details
CVE-2021-38705	ClinicCases 7.3.3 is affected by Cross-Site Request Forgery (CSRF). A successful attack would consist of an authenticated user following a malicious link, resulting in arbitrary actions being carried out with the privilege level of the targeted user. This can be exploited to create a secondary administrator account for the attacker.	8.8	More Details
CVE-2021-37219	HashiCorp Consul and Consul Enterprise 1.10.1 Raft RPC layer allows non-server agents with a valid certificate signed by the same CA to access server-only functionality, enabling privilege escalation. Fixed in 1.8.15, 1.9.9 and 1.10.2.	8.8	More Details
CVE-2021-24303	The JiangQie Official Website Mini Program WordPress plugin before 1.1.1 does not escape or validate the id GET parameter before using it in SQL statements, leading to SQL injection issues	8.8	More Details
CVE-2021-28550	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by a Use After Free 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.	8.8	More Details
CVE-2021-30623	Chromium: CVE-2021-30623 Use after free in Bookmarks	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28553	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by an Use After Free 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.	8.8	More Details
CVE-2021-37218	HashiCorp Nomad and Nomad Enterprise Raft RPC layer allows non-server agents with a valid certificate signed by the same CA to access server-only functionality, enabling privilege escalation. Fixed in 1.0.10 and 1.1.4.	8.8	More Details
CVE-2021-36162	Apache Dubbo supports various rules to support configuration override or traffic routing (called routing in Dubbo). These rules are loaded into the configuration center (eg: Zookeeper, Nacos, ...) and retrieved by the customers when making a request in order to find the right endpoint. When parsing these YAML rules, Dubbo customers will use SnakeYAML library to load the rules which by default will enable calling arbitrary constructors. An attacker with access to the configuration center he will be able to poison the rule so when retrieved by the consumers, it will get RCE on all of them. This was fixed in Dubbo 2.7.13, 3.0.2	8.8	More Details
CVE-2021-34435	In Eclipse Theia 0.3.9 to 1.8.1, the "mini-browser" extension allows a user to preview HTML files in an iframe inside the IDE. But with the way it is made it is possible for a previewed HTML file to trigger an RCE. This exploit only happens if a user previews a malicious file..	8.8	More Details
CVE-2021-38841	Remote Code Execution can occur in Simple Water Refilling Station Management System 1.0 via the System Logo option on the system_info page in classes/SystemSettings.php with an update_settings action.	8.8	More Details
CVE-2021-28139	The Bluetooth Classic implementation in Espressif ESP-IDF 4.4 and earlier does not properly restrict the Feature Page upon reception of an LMP Feature Response Extended packet, allowing attackers in radio range to trigger arbitrary code execution in ESP32 via a crafted Extended Features bitfield payload.	8.8	More Details
CVE-2021-28560	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are 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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39279	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP-323-JP-CT-T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.	8.8	More Details
CVE-2021-28564	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by an Out-of-bounds Write vulnerability within the ImageTool component. 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.	8.8	More Details
CVE-2020-7832	A vulnerability (improper input validation) in the DEXT5 Upload solution allows an unauthenticated attacker to download and execute an arbitrary file via AddUploadFile, SetSelectItem, DoOpenFile function.(CVE-2020-7832)	8.8	More Details
CVE-2021-30607	Chromium: CVE-2021-30607 Use after free in Permissions	8.8	More Details
CVE-2021-30606	Chromium: CVE-2021-30606 Use after free in Blink	8.8	More Details
CVE-2021-28561	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are 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.	8.8	More Details
CVE-2021-30622	Chromium: CVE-2021-30622 Use after free in WebApp Installs	8.8	More Details
CVE-2021-30616	Chromium: CVE-2021-30616 Use after free in Media	8.8	More Details
CVE-2021-30614	Chromium: CVE-2021-30614 Heap buffer overflow in TabStrip	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38703	Wireless devices running certain Arcadyan-derived firmware (such as KPN Experia WiFi 1.00.15) do not properly sanitise user input to the syslog configuration form. An authenticated remote attacker could leverage this to alter the device configuration and achieve remote code execution. This can be exploited in conjunction with CVE-2021-20090.	8.8	More Details
CVE-2021-30613	Chromium: CVE-2021-30613 Use after free in Base internals	8.8	More Details
CVE-2021-30612	Chromium: CVE-2021-30612 Use after free in WebRTC	8.8	More Details
CVE-2021-30611	Chromium: CVE-2021-30611 Use after free in WebRTC	8.8	More Details
CVE-2021-35508	NMSAccess32.exe in TeraRecon AQNetClient 4.4.13 allows attackers to execute a malicious binary with SYSTEM privileges via a low-privileged user account. To exploit this, a low-privileged user must change the service configuration or overwrite the binary service.	8.8	More Details
CVE-2021-30620	Chromium: CVE-2021-30620 Insufficient policy enforcement in Blink	8.8	More Details
CVE-2021-39181	OpenOlat is a web-based learning management system (LMS). Prior to version 15.3.18, 15.5.3, and 16.0.0, using a prepared import XML file (e.g. a course) any class on the Java classpath can be instantiated, including spring AOP bean factories. This can be used to execute code arbitrary code by the attacker. The attack requires an OpenOlat user account with the authoring role. It can not be exploited by unregistered users. The problem is fixed in versions 15.3.18, 15.5.3, and 16.0.0. There are no known workarounds aside from upgrading.	8.8	More Details
CVE-2021-30610	Chromium: CVE-2021-30610 Use after free in Extensions API	8.8	More Details
CVE-2021-40385	An issue was discovered in the server software in Kaseya Unitrends Backup Software before 10.5.5-2. There is a privilege escalation from read-only user to admin.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40387	An issue was discovered in the server software in Kaseya Unitrends Backup Software before 10.5.5-2. There is authenticated remote code execution.	8.8	More Details
CVE-2021-30609	Chromium: CVE-2021-30609 Use after free in Sign-In	8.8	More Details
CVE-2021-30608	Chromium: CVE-2021-30608 Use after free in Web Share	8.8	More Details
CVE-2020-7865	A vulnerability(improper input validation) in the ExECM CoreB2B solution allows an unauthenticated attacker to download and execute an arbitrary file via httpDownload function. A successful exploit could allow the attacker to hijack vulnerable system.	8.8	More Details
CVE-2021-38142	Barco MirrorOp Windows Sender before 2.5.3.65 uses cleartext HTTP and thus allows rogue software upgrades. An attacker on the local network can achieve remote code execution on any computer that tries to update Windows Sender due to the fact that the upgrade mechanism is not secured (is not protected with TLS).	8.8	More Details
CVE-2021-30355	Amazon Kindle e-reader prior to and including version 5.13.4 improperly manages privileges, allowing the framework user to elevate privileges to root.	8.6	More Details
CVE-2021-30354	Amazon Kindle e-reader prior to and including version 5.13.4 contains an Integer Overflow that leads to a Heap-Based Buffer Overflow in function CJBig2Image::expand() and results in a memory corruption that leads to code execution when parsing a crafted PDF book.	8.6	More Details
CVE-2021-23428	This affects all versions of package elFinder.NetCore. The Path.Combine(...) method is used to create an absolute file path. Due to missing sanitation of the user input and a missing check of the generated path its possible to escape the Files directory via path traversal	8.6	More Details
CVE-2021-23427	This affects all versions of package elFinder.NetCore. The ExtractAsync function within the FileSystem is vulnerable to arbitrary extraction due to insufficient validation.	8.6	More Details
CVE-2021-36032	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36020	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability in the 'City' field. An unauthenticated attacker can trigger a specially crafted script to achieve remote code execution.	8.2	More Details
CVE-2021-40143	Sonatype Nexus Repository 3.x through 3.33.1-01 is vulnerable to an HTTP header injection. By sending a crafted HTTP request, a remote attacker may disclose sensitive information or request external resources from a vulnerable instance.	8.2	More Details
CVE-2021-32800	Nextcloud server is an open source, self hosted personal cloud. In affected versions an attacker is able to bypass Two Factor Authentication in Nextcloud. Thus knowledge of a password, or access to a WebAuthN trusted device of a user was sufficient to gain access to an account. It is recommended that the Nextcloud Server is upgraded to 20.0.12, 21.0.4 or 22.1.0. There are no workaround for this vulnerability.	8.1	More Details
CVE-2021-37725	A remote cross-site request forgery (csrf) vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.8.0.1, 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	8.1	More Details
CVE-2021-40378	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. /cgi-bin/support/killps.cgi deletes all data from the device.	8.1	More Details
CVE-2021-39166	Pimcore is an open source data & experience management platform. Prior to version 10.1.2, text-values were not properly escaped before printed in the version preview. This allowed XSS by authenticated users with access to the resources. This issue is patched in Pimcore version 10.1.2.	8.0	More Details
CVE-2021-36043	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a blind SSRF vulnerability in the bundled dotmailer extension. An attacker with admin privileges could abuse this to achieve remote code execution should Redis be enabled.	8.0	More Details
CVE-2021-39170	Pimcore is an open source data & experience management platform. Prior to version 10.1.2, an authenticated user could add XSS code as a value of custom metadata on assets. There is a patch for this issue in Pimcore version 10.1.2. As a workaround, users may apply the patch manually.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7877	A buffer overflow issue was discovered in ZOOK solution(remote administration tool) through processing 'ConnectMe' command while parsing a crafted OUTERIP value because of missing boundary check. This vulnerability allows the attacker to execute remote arbitrary command.	8.0	More Details
CVE-2021-35267	NTFS-3G versions < 2021.8.22, a stack buffer overflow can occur when correcting differences in the MFT and MFTMirror allowing for code execution or escalation of privileges when setuid-root.	7.8	More Details
CVE-2021-35266	In NTFS-3G versions < 2021.8.22, when a specially crafted NTFS inode pathname is supplied in an NTFS image a heap buffer overflow can occur resulting in memory disclosure, denial of service and even code execution.	7.8	More Details
CVE-2021-33287	In NTFS-3G versions < 2021.8.22, when specially crafted NTFS attributes are read in the function ntfs_attr_pread_i, a heap buffer overflow can occur and allow for writing to arbitrary memory or denial of service of the application.	7.8	More Details
CVE-2021-33286	In NTFS-3G versions < 2021.8.22, when a specially crafted unicode string is supplied in an NTFS image a heap buffer overflow can occur and allow for code execution.	7.8	More Details
CVE-2021-35993	Adobe After Effects version 18.2.1 (and earlier) is affected by an out-of-bounds Write 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-2021-35268	In NTFS-3G versions < 2021.8.22, when a specially crafted NTFS inode is loaded in the function ntfs_inode_real_open, a heap buffer overflow can occur allowing for code execution and escalation of privileges.	7.8	More Details
CVE-2021-35269	NTFS-3G versions < 2021.8.22, when a specially crafted NTFS attribute from the MFT is setup in the function ntfs_attr_setup_flag, a heap buffer overflow can occur allowing for code execution and escalation of privileges.	7.8	More Details
CVE-2021-35994	Adobe After Effects version 18.2.1 (and earlier) is affected by an out-of-bounds Write 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 Number	Description	Base Score	Reference
CVE-2021-33289	In NTFS-3G versions < 2021.8.22, when a specially crafted MFT section is supplied in an NTFS image a heap buffer overflow can occur and allow for code execution.	7.8	More Details
CVE-2021-33285	In NTFS-3G versions < 2021.8.22, when a specially crafted NTFS attribute is supplied to the function ntfs_get_attribute_value, a heap buffer overflow can occur allowing for memory disclosure or denial of service. The vulnerability is caused by an out-of-bound buffer access which can be triggered by mounting a crafted ntfs partition. The root cause is a missing consistency check after reading an MFT record : the "bytes_in_use" field should be less than the "bytes_allocated" field. When it is not, the parsing of the records proceeds into the wild.	7.8	More Details
CVE-2021-21086	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (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-2021-22775	A CWE-427: Uncontrolled Search Path Element vulnerability exists in GP-Pro EX,V4.09.250 and prior, that could cause local code execution with elevated privileges when installing the software.	7.8	More Details
CVE-2021-32568	mrdoc is vulnerable to Deserialization of Untrusted Data	7.8	More Details
CVE-2021-36744	Trend Micro Security (Consumer) 2021 and 2020 are vulnerable to a directory junction vulnerability which could allow an attacker to exploit the system to escalate privileges and create a denial of service.	7.8	More Details
CVE-2021-3770	vim is vulnerable to Heap-based Buffer Overflow	7.8	More Details
CVE-2021-36017	Adobe After Effects version 18.2.1 (and earlier) is 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 Number	Description	Base Score	Reference
CVE-2021-35996	Adobe After Effects version 18.2.1 (and earlier) is 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-2021-36235	An issue was discovered in Ivanti Workspace Control before 10.6.30.0. A locally authenticated user with low privileges can bypass File and Folder Security by leveraging an unspecified attack vector. As a result, the attacker can start applications with elevated privileges.	7.8	More Details
CVE-2021-39251	A crafted NTFS image can cause a NULL pointer dereference in ntfs_extent_inode_open in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-36059	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-36069	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-36068	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-36067	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-36065	Adobe Photoshop versions 21.2.10 (and earlier) and 22.4.3 (and earlier) are affected by a heap-based buffer overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-36064	XMP Toolkit version 2020.1 (and earlier) is affected by a Buffer Underflow vulnerability which could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39260	A crafted NTFS image can cause an out-of-bounds access in ntfs_inode_sync_standard_information in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-39261	A crafted NTFS image can cause a heap-based buffer overflow in ntfs_compressed_pwrite in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-39262	A crafted NTFS image can cause an out-of-bounds access in ntfs_decompress in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-39263	A crafted NTFS image can trigger a heap-based buffer overflow, caused by an unsanitized attribute in ntfs_get_attribute_value, in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-39259	A crafted NTFS image can trigger an out-of-bounds access, caused by an unsanitized attribute length in ntfs_inode_lookup_by_name, in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-36055	XMP Toolkit SDK versions 2020.1 (and earlier) are affected by a use-after-free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-36052	XMP Toolkit version 2020.1 (and earlier) is affected by a memory corruption vulnerability, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-36050	XMP Toolkit SDK version 2020.1 (and earlier) is affected by a buffer overflow vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file.	7.8	More Details
CVE-2021-36049	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-36048	XMP Toolkit SDK version 2020.1 (and earlier) is affected by an Improper Input Validation vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36047	XMP Toolkit SDK version 2020.1 (and earlier) is affected by an Improper Input Validation vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file.	7.8	More Details
CVE-2021-36046	XMP Toolkit version 2020.1 (and earlier) is affected by a memory corruption vulnerability, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-39373	Samsung Drive Manager 2.0.104 on Samsung H3 devices allows attackers to bypass intended access controls on disk management. WideCharToMultiByte, WideCharStr, and MultiByteStr can contribute to password exposure.	7.8	More Details
CVE-2021-36070	Adobe Media Encoder version 15.1 (and earlier) is affected by an improper memory access vulnerability when parsing a crafted .SVG file. An attacker could leverage this vulnerability to execute code 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-2021-36066	Adobe Photoshop versions 21.2.10 (and earlier) and 22.4.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-39252	A crafted NTFS image can cause an out-of-bounds read in ntfs_ie_lookup in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-36073	Adobe Bridge version 11.1 (and earlier) is affected by a heap-based buffer overflow vulnerability when parsing a crafted .SGI file. An attacker could leverage this vulnerability to execute code 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-2021-36076	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-36075	Adobe Bridge version 11.1 (and earlier) is affected by a Buffer Overflow vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39256	A crafted NTFS image can cause a heap-based buffer overflow in ntfs_inode_lookup_by_name in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-36078	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-39258	A crafted NTFS image can cause out-of-bounds reads in ntfs_attr_find and ntfs_external_attr_find in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-36079	Adobe Bridge version 11.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted .SGI file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2021-39255	A crafted NTFS image can trigger an out-of-bounds read, caused by an invalid attribute in ntfs_attr_find_in_attrdef, in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-39816	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-39817	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-39847	XMP Toolkit SDK version 2020.1 (and earlier) is affected by a stack-based buffer overflow vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file.	7.8	More Details
CVE-2021-36072	Adobe Bridge versions 11.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39254	A crafted NTFS image can cause an integer overflow in memmove, leading to a heap-based buffer overflow in the function ntfs_attr_record_resize, in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-39253	A crafted NTFS image can cause an out-of-bounds read in ntfs_runlists_merge_i in NTFS-3G < 2021.8.22.	7.8	More Details
CVE-2021-39195	Misskey is an open source, decentralized microblogging platform. In affected versions a Server-Side Request Forgery vulnerability exists in "Upload from URL" and remote attachment handling. This could result in the disclosure of non-public information within the internal network. This has been fixed in 12.90.0. However, if you are using a proxy, you will need to take additional measures. As a workaround this exploit may be avoided by appropriately restricting access to private networks from the host where the application is running.	7.7	More Details
CVE-2021-39196	pcapture is an open source dumpcap web service interface . In affected versions this vulnerability allows an authenticated but unprivileged user to use the REST API to capture and download packets with no capture filter and without adequate permissions. This is important because the capture filters can effectively limit the scope of information that a user can see in the data captures. If no filter is present, then all data on the local network segment where the program is running can be captured and downloaded. v3.12 fixes this problem. There is no workaround, you must upgrade to v3.12 or greater.	7.7	More Details
CVE-2021-38616	In Eigen NLP 3.10.1, a lack of access control on the /auth/v1/user/{user-guid}/ user edition endpoint could permit any logged-in user to increase their own permissions via a user_permissions array in a PATCH request. A guest user could modify other users' profiles and much more.	7.6	More Details
CVE-2021-40524	In Pure-FTPd before 1.0.50, an incorrect max_filesize quota mechanism in the server allows attackers to upload files of unbounded size, which may lead to denial of service or a server hang. This occurs because a certain greater-than-zero test does not anticipate an initial -1 value. (Versions 1.0.23 through 1.0.49 are affected.)	7.5	More Details
CVE-2021-36044	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An unauthenticated attacker could abuse this vulnerability to cause a server-side denial-of-service using a GraphQL field.	7.5	More Details
CVE-2020-19752	The find_color_or_error function in gifsicle 1.92 contains a NULL pointer dereference.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31796	An inadequate encryption vulnerability discovered in CyberArk Credential Provider before 12.1 may lead to Information Disclosure. An attacker may realistically have enough information that the number of possible keys (for a credential file) is only one, and the number is usually not higher than 2^36.	7.5	More Details
CVE-2021-40523	In Contiki 3.0, Telnet option negotiation is mishandled. During negotiation between a server and a client, the server may fail to give the WILL/WONT or DO/DONT response for DO and WILL commands because of improper handling of exception condition, which leads to property violations and denial of service. Specifically, a server sometimes sends no response, because a fixed buffer space is available for all responses and that space may have been exhausted.	7.5	More Details
CVE-2020-19768	A lack of target address verification in the selfdestructs() function of ICOVO 1.0 allows attackers to steal tokens from victim users via a crafted script.	7.5	More Details
CVE-2021-39109	The renderWidgetResource resource in Atlasian Atlasboard before version 1.1.9 allows remote attackers to read arbitrary files via a path traversal vulnerability.	7.5	More Details
CVE-2020-9000	An issue was discovered in iPortalis iCS 7.1.13.0. Attackers can send a sequence of requests to rapidly cause .NET Input Validation errors. This increases the size of the log file on the remote server until memory is exhausted, therefore consuming the maximum amount of resources (triggering a denial of service condition).	7.5	More Details
CVE-2021-33582	Cyrus IMAP before 3.4.2 allows remote attackers to cause a denial of service (multiple-minute daemon hang) via input that is mishandled during hash-table interaction. Because there are many insertions into a single bucket, strcmp becomes slow. This is fixed in 3.4.2, 3.2.8, and 3.0.16.	7.5	More Details
CVE-2020-9002	An issue was discovered in iPortalis iCS 7.1.13.0. An attacker can gain privileges by intercepting a request and changing UserRoleKey=COMPANY_ADMIN to UserRoleKey=DOMAIN_ADMIN (to achieve Domain Administrator access).	7.5	More Details
CVE-2020-19769	A lack of target address verification in the BurnMe() function of Rob The Bank 1.0 allows attackers to steal tokens from victim users via a crafted script.	7.5	More Details
CVE-2021-40380	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. cameralist.cgi and setcamera.cgi disclose credentials.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19767	A lack of target address verification in the destroycontract() function of 0xRACER 1.0 allows attackers to steal tokens from victim users via a crafted script.	7.5	More Details
CVE-2021-40381	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. index_MJpeg.cgi allows video access.	7.5	More Details
CVE-2020-19766	The time check operation of PepeAuctionSale 1.0 can be rendered ineffective by assigning a large number to the _duration variable, compromising access control to the application.	7.5	More Details
CVE-2020-19765	An issue in the noReentrance() modifier of the Ethereum-based contract Accounting 1.0 allows attackers to carry out a reentrancy attack.	7.5	More Details
CVE-2021-39500	Eyoucms 1.5.4 is vulnerable to Directory Traversal. Due to a lack of input data sanitizaton in param tpldir, filename, type, nid an attacker can inject "../" to escape and write file to writeable directories.	7.5	More Details
CVE-2021-37628	Nextcloud Richdocuments is an open source collaborative office suite. In affected versions the File Drop features ("Upload Only" public link shares in Nextcloud) can be bypassed using the Nextcloud Richdocuments app. An attacker was able to read arbitrary files in such a share. It is recommended that the Nextcloud Richdocuments is upgraded to 3.8.4 or 4.2.1. If upgrading is not possible then it is recommended to disable the Richdocuments application.	7.5	More Details
CVE-2021-36030	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability during the checkout process. An unauthenticated attacker can leverage this vulnerability to alter the price of items.	7.5	More Details
CVE-2021-23437	The package pillow 5.2.0 and before 8.3.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via the getrgb function.	7.5	More Details
CVE-2021-40516	WeeChat before 3.2.1 allows remote attackers to cause a denial of service (crash) via a crafted WebSocket frame that trigger an out-of-bounds read in plugins/relay/relay-websocket.c in the Relay plugin.	7.5	More Details
CVE-2020-19750	An issue was discovered in gpac 0.8.0. The strdup function in box_code_base.c has a heap-based buffer over-read.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40382	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. mjpegStreamer.cgi allows video screenshot access.	7.5	More Details
CVE-2020-19131	Buffer Overflow in LibTiff v4.0.10 allows attackers to cause a denial of service via the "invertImage()" function in the component "tiffcrop".	7.5	More Details
CVE-2021-33928	Buffer overflow vulnerability in function pool_installable in src/repo.h in libsolv before 0.7.17 allows attackers to cause a Denial of Service.	7.5	More Details
CVE-2021-33929	Buffer overflow vulnerability in function pool_disabled_solvable in src/repo.h in libsolv before 0.7.17 allows attackers to cause a Denial of Service.	7.5	More Details
CVE-2021-33930	Buffer overflow vulnerability in function pool_installable_whatprovides in src/repo.h in libsolv before 0.7.17 allows attackers to cause a Denial of Service.	7.5	More Details
CVE-2021-33938	Buffer overflow vulnerability in function prune_to_recommended in src/policy.c in libsolv before 0.7.17 allows attackers to cause a Denial of Service.	7.5	More Details
CVE-2021-39187	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to version 4.10.3, Parse Server crashes when if a query request contains an invalid value for the `explain` option. This is due to a bug in the MongoDB Node.js driver which throws an exception that Parse Server cannot catch. There is a patch for this issue in version 4.10.3. No workarounds aside from upgrading are known to exist.	7.5	More Details
CVE-2020-13929	Authentication bypass vulnerability in Apache Zeppelin allows an attacker to bypass Zeppelin authentication mechanism to act as another user. This issue affects Apache Zeppelin Apache Zeppelin version 0.9.0 and prior versions.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22792	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure[a] Control Expert, including all Unity Pro versions (former name of EcoStruxure[a] Control Expert, all versions), PLC Simulator for EcoStruxure[a] Process Expert including all HDCS versions (former name of EcoStruxure[a] Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	7.5	More Details
CVE-2020-20340	A SQL injection vulnerability in the 4.edu.php\conn\function.php component of S-CMS v1.0 allows attackers to access sensitive database information.	7.5	More Details
CVE-2021-40379	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. rstp://.../medias2 does not require authorization.	7.5	More Details
CVE-2020-20341	YzmCMS v5.5 contains a server-side request forgery (SSRF) in the grab_image() function.	7.5	More Details
CVE-2021-33484	An issue was discovered in CommentsService.ashx in OnyakTech Comments Pro 3.8. An attacker can download a copy of the installer, decompile it, and discover a hardcoded IV used to encrypt the username and userid in the comment POST request. Additionally, the attacker can decrypt the encrypted encryption key (sent as a parameter in the comment form request) by setting this encrypted value as the username, which will appear on the comment page in its decrypted form. Using these two values (combined with the encryption functionality discovered in the decompiled installer), the attacker can encrypt another user's ID and username. These values can be used as part of the comment posting request in order to spoof the user.	7.5	More Details
CVE-2021-24394	An id GET parameter of the Easy Testimonial Manager WordPress plugin through 1.2.0 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37724	A remote arbitrary command execution vulnerability was discovered in Aruba Operating System Software version(s): Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.16. Aruba has released patches for ArubaOS that address this security vulnerability.	7.2	More Details
CVE-2021-37723	A remote arbitrary command execution vulnerability was discovered in Aruba Operating System Software version(s): Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.16. Aruba has released patches for ArubaOS that address this security vulnerability.	7.2	More Details
CVE-2021-37722	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	7.2	More Details
CVE-2021-37721	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	7.2	More Details
CVE-2021-37720	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	7.2	More Details
CVE-2021-24392	An id GET parameter of the WordPress Membership SwiftCloud.io WordPress plugin through 1.0 is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	7.2	More Details
CVE-2021-24393	A c GET parameter of the Comment Highlighter WordPress plugin through 0.13 is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	7.2	More Details
CVE-2021-37717	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.6; Prior to 8.7.1.4, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24390	A proid GET parameter of the WordPress支付宝Alipayl财付通Tenpayl贝宝PayPal集成插件 WordPress plugin through 3.7.2 is not sanitised, properly escaped or validated before inserting to a SQL statement not delimited by quotes, leading to SQL injection.	7.2	More Details
CVE-2021-37719	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	7.2	More Details
CVE-2021-24395	The editid GET parameter of the Embed Youtube Video WordPress plugin through 1.0 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	7.2	More Details
CVE-2021-39503	PHPMyWind 5.6 is vulnerable to Remote Code Execution. Becase input is filtered without "<, >, ?, =, `,...." In WriteConfig() function, an attacker can inject php code to /include/config.cache.php file.	7.2	More Details
CVE-2021-37718	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.6; Prior to 8.7.1.4, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	7.2	More Details
CVE-2021-37145	A command-injection vulnerability in an authenticated Telnet connection in Poly (formerly Polycom) CX5500 and CX5100 1.3.5 leads an attacker to Privilege Escalation and Remote Code Execution capability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.2	More Details
CVE-2021-22793	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exist in AccuSine PCS+ / PFV+ (Versions prior to V1.6.7) and AccuSine PCSn (Versions prior to V2.2.4) that could allow an authenticated attacker to access the device via FTP protocol.	7.2	More Details
CVE-2021-36031	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a Path Traversal vulnerability via the `theme[preview_image]` parameter. An attacker with admin privileges could leverage this vulnerability to achieve remote code execution.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39115	Affected versions of Atlassian Jira Service Management Server and Data Center allow remote attackers with "Jira Administrators" access to execute arbitrary Java code or run arbitrary system commands via a Server_Side Template Injection vulnerability in the Email Template feature. The affected versions are before version 4.13.9, and from version 4.14.0 before 4.18.0.	7.2	More Details
CVE-2021-38312	The Gutenberg Template Library & Redux Framework plugin <= 4.2.11 for WordPress used an incorrect authorization check in the REST API endpoints registered under the “redux/v1/templates/” REST Route in “redux-templates/classes/class-api.php”. The `permissions_callback` used in this file only checked for the `edit_posts` capability which is granted to lower-privileged users such as contributors, allowing such users to install arbitrary plugins from the WordPress repository and edit arbitrary posts.	7.1	More Details
CVE-2021-40490	A race condition was discovered in ext4_write_inline_data_end in fs/ext4/inline.c in the ext4 subsystem in the Linux kernel through 5.13.13.	7.0	More Details
CVE-2021-34149	The Bluetooth Classic implementation on the Texas Instruments CC256XCQFN-EM does not properly handle the reception of continuous LMP_AU_Rand packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after the paging procedure.	6.5	More Details
CVE-2021-34148	The Bluetooth Classic implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 devices does not properly handle the reception of LMP_max_slot with a greater ACL Length after completion of the LMP setup procedure, allowing attackers in radio range to trigger a denial of service (firmware crash) via a crafted LMP packet.	6.5	More Details
CVE-2021-34147	The Bluetooth Classic implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 does not properly handle the reception of a malformed LMP timing accuracy response followed by multiple reconnections to the link slave, allowing attackers to exhaust device BT resources and eventually trigger a crash via multiple attempts of sending a crafted LMP timing accuracy response followed by a sudden reconnection with a random BDAddress.	6.5	More Details
CVE-2021-34146	The Bluetooth Classic implementation in the Cypress CYW920735Q60EVB does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and restart (crash) of the device by flooding it with LMP_AU_Rand packets after the paging procedure.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34143	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.	6.5	More Details
CVE-2021-31786	The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that matches the original connected host.	6.5	More Details
CVE-2021-31785	The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication.	6.5	More Details
CVE-2021-30619	Chromium: CVE-2021-30619 UI Spoofing in Autofill	6.5	More Details
CVE-2021-30621	Chromium: CVE-2021-30621 UI Spoofing in Autofill	6.5	More Details
CVE-2021-31610	The Bluetooth Classic implementation on AB32VG1 devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (either restart or deadlock the device) by flooding a device with LMP_AU_rand data.	6.5	More Details
CVE-2021-31609	The Bluetooth Classic implementation in Silicon Labs iWRAP 6.3.0 and earlier does not properly handle the reception of an oversized LMP packet greater than 17 bytes, allowing attackers in radio range to trigger a crash in WT32i via a crafted LMP packet.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34150	The Bluetooth Classic implementation on Bluetrum AB5301A devices with unknown firmware versions does not properly handle the reception of oversized DM1 LMP packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.	6.5	More Details
CVE-2021-34144	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.	6.5	More Details
CVE-2021-33831	api/account/register in the TH Wildau COVID-19 Contact Tracing application through 2021-09-01 has Incorrect Access Control. An attacker can interfere with tracing of infection chains by creating 500 random users within 2500 seconds.	6.5	More Details
CVE-2021-31613	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet.	6.5	More Details
CVE-2021-28155	The Bluetooth Classic implementation on JBL TUNE500BT devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and shutdown a device by flooding the target device with LMP Feature Response data.	6.5	More Details
CVE-2021-31612	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet.	6.5	More Details
CVE-2019-5318	A remote cross-site request forgery (csrf) vulnerability was discovered in Aruba Operating System Software version(s): 6.x.x.x: all versions, 8.x.x.x: all versions prior to 8.8.0.0. Aruba has released patches for ArubaOS that address this security vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38698	HashiCorp Consul and Consul Enterprise 1.10.1 Txn.Apply endpoint allowed services to register proxies for other services, enabling access to service traffic. Fixed in 1.8.15, 1.9.9 and 1.10.2.	6.5	More Details
CVE-2021-28135	The Bluetooth Classic implementation in Espressif ESP-IDF 4.4 and earlier does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (crash) in ESP32 by flooding the target device with LMP Feature Response data.	6.5	More Details
CVE-2021-40352	OpenEMR 6.0.0 has a pnotes_print.php?noteid= Insecure Direct Object Reference vulnerability via which an attacker can read the messages of all users.	6.5	More Details
CVE-2021-36012	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a business logic error in the placeOrder graphql mutation. An authenticated attacker can leverage this vulnerability to altar the price of an item.	6.5	More Details
CVE-2021-36026	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a stored cross-site scripting vulnerability in the customer address upload feature that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	6.5	More Details
CVE-2021-36027	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a stored cross-site scripting vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	6.5	More Details
CVE-2021-36037	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper improper authorization vulnerability. An authenticated attacker could leverage this vulnerability to achieve sensitive information disclosure.	6.5	More Details
CVE-2021-36038	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability in the Multishipping Module. An authenticated attacker could leverage this vulnerability to achieve sensitive information disclosure.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36039	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability via the `quoteId` parameter. An attacker can abuse this vulnerability to disclose sensitive information.	6.5	More Details
CVE-2021-37631	Deck is an open source kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. In affected versions the Deck application didn't properly check membership of users in a Circle. This allowed other users in the instance to gain access to boards that have been shared with a Circle, even if the user was not a member of the circle. It is recommended that Nextcloud Deck is upgraded to 1.5.1, 1.4.4 or 1.2.9. If you are unable to update it is advised to disable the Deck plugin.	6.5	More Details
CVE-2021-37630	Nextcloud Circles is an open source social network built for the nextcloud ecosystem. In affected versions the Nextcloud Circles application allowed any user to join any "Secret Circle" without approval by the Circle owner leaking private information. It is recommended that Nextcloud Circles is upgraded to 0.19.15, 0.20.11 or 0.21.4. There are no workarounds for this issue.	6.5	More Details
CVE-2020-20343	WTCMS 1.0 contains a cross-site request forgery (CSRF) vulnerability in the index.php?g=admin&m=nav&a=add_post component that allows attackers to arbitrarily add articles in the administrator background.	6.5	More Details
CVE-2021-37729	A remote path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0-2.2.0.4; Prior to 8.7.1.3, 8.6.0.9, 8.5.0.12, 8.3.0.16, 6.5.4.19, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	6.5	More Details
CVE-2021-37728	A remote path traversal vulnerability was discovered in Aruba Operating System Software version(s): Prior to 8.8.0.1, 8.7.1.4, 8.6.0.11, 8.5.0.13. Aruba has released patches for ArubaOS that address this security vulnerability.	6.5	More Details
CVE-2021-3758	bookstack is vulnerable to Server-Side Request Forgery (SSRF)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22789	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure[a] Control Expert, including all Unity Pro versions (former name of EcoStruxure[a] Control Expert, all versions), PLC Simulator for EcoStruxure[a] Process Expert including all HDCS versions (former name of EcoStruxure[a] Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	6.5	More Details
CVE-2021-22790	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure[a] Control Expert, including all Unity Pro versions (former name of EcoStruxure[a] Control Expert, all versions), PLC Simulator for EcoStruxure[a] Process Expert including all HDCS versions (former name of EcoStruxure[a] Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	6.5	More Details
CVE-2021-28136	The Bluetooth Classic implementation in Espressif ESP-IDF 4.4 and earlier does not properly handle the reception of multiple LMP IO Capability Request packets during the pairing process, allowing attackers in radio range to trigger memory corruption (and consequently a crash) in ESP32 via a replayed (duplicated) LMP packet.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22791	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure[a] Control Expert, including all Unity Pro versions (former name of EcoStruxure[a] Control Expert, all versions), PLC Simulator for EcoStruxure[a] Process Expert including all HDCS versions (former name of EcoStruxure[a] Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	6.5	More Details
CVE-2021-30615	Chromium: CVE-2021-30615 Cross-origin data leak in Navigation	6.5	More Details
CVE-2021-39192	Ghost is a Node.js content management system. An error in the implementation of the limits service between versions 4.0.0 and 4.9.4 allows all authenticated users (including contributors) to view admin-level API keys via the integrations API endpoint, leading to a privilege escalation vulnerability. This issue is patched in Ghost version 4.10.0. As a workaround, disable all non-Administrator accounts to prevent API access. It is highly recommended to regenerate all API keys after patching or applying the workaround.	6.5	More Details
CVE-2021-30617	Chromium: CVE-2021-30617 Policy bypass in Blink	6.5	More Details
CVE-2021-25735	A security issue was discovered in kube-apiserver that could allow node updates to bypass a Validating Admission Webhook. Clusters are only affected by this vulnerability if they run a Validating Admission Webhook for Nodes that denies admission based at least partially on the old state of the Node object. Validating Admission Webhook does not observe some previous fields.	6.5	More Details
CVE-2021-40491	The ftp client in GNU Inetutils before 2.2 does not validate addresses returned by PASV/LSPV responses to make sure they match the server address. This is similar to CVE-2020-8284 for curl.	6.5	More Details
CVE-2021-38615	In Eigen NLP 3.10.1, a lack of access control on the /auth/v1/sso/config/ SSO configuration endpoint allows any logged-in user (guest, standard, or admin) to view and modify information.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39197	better_errors is an open source replacement for the standard Rails error page with more information rich error pages. It is also usable outside of Rails in any Rack app as Rack middleware. better_errors prior to 2.8.0 did not implement CSRF protection for its internal requests. It also did not enforce the correct "Content-Type" header for these requests, which allowed a cross-origin "simple request" to be made without CORS protection. These together left an application with better_errors enabled open to cross-origin attacks. As a developer tool, better_errors documentation strongly recommends addition only to the `development` bundle group, so this vulnerability should only affect development environments. Please ensure that your project limits better_errors to the `development` group (or the non-Rails equivalent). Starting with release 2.8.x, CSRF protection is enforced. It is recommended that you upgrade to the latest release, or minimally to "~> 2.8.3". There are no known workarounds to mitigate the risk of using older releases of better_errors.	6.3	More Details
CVE-2021-24006	An improper access control vulnerability in FortiManager versions 6.4.0 to 6.4.3 may allow an authenticated attacker with a restricted user profile to access the SD-WAN Orchestrator panel via directly visiting its URL.	6.3	More Details
CVE-2021-37731	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0-2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	6.2	More Details
CVE-2021-39499	A Cross-site scripting (XSS) vulnerability in Users in Qiong ICP EyouCMS 1.5.4 allows remote attackers to inject arbitrary web script or HTML via the `title` parameter in bind_email function.	6.1	More Details
CVE-2021-39501	EyouCMS 1.5.4 is vulnerable to Open Redirect. An attacker can redirect a user to a malicious url via the Logout function.	6.1	More Details
CVE-2021-24588	The SMS Alert Order Notifications WordPress plugin before 3.4.7 is affected by a cross site scripting (XSS) vulnerability in the plugin's setting page.	6.1	More Details
CVE-2021-24435	The iframe-font-preview.php file of the titan-framework does not properly escape the font-weight and font-family GET parameters before outputting them back in an href attribute, leading to Reflected Cross-Site Scripting issues	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34732	A vulnerability in the web-based management interface of Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	6.1	More Details
CVE-2021-40492	A reflected XSS vulnerability exists in multiple pages in version 22 of the Gibbon application that allows for arbitrary execution of JavaScript (gibbonCourseClassID, gibbonPersonID, subpage, currentDate, or allStudents to index.php).	6.1	More Details
CVE-2021-39322	The Easy Social Icons plugin <= 3.0.8 for WordPress echoes out the raw value of `$_SERVER['PHP_SELF']` in its main file. On certain configurations including Apache+modPHP this makes it possible to use it to perform a reflected Cross-Site Scripting attack by injecting malicious code in the request path.	6.1	More Details
CVE-2021-26436	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	6.1	More Details
CVE-2021-39285	A XSS vulnerability exists in Versa Director Release: 16.1R2 Build: S8. An attacker can use the administration web interface URL to create a XSS based attack.	6.1	More Details
CVE-2021-39320	The underConstruction plugin <= 1.18 for WordPress echoes out the raw value of `$GLOBALS['PHP_SELF']` in the ucOptions.php file. On certain configurations including Apache+modPHP, this makes it possible to use it to perform a reflected Cross-Site Scripting attack by injecting malicious code in the request path.	6.1	More Details
CVE-2021-38123	Open Redirect vulnerability in Micro Focus Network Automation, affecting Network Automation versions 10.4x, 10.5x, 2018.05, 2018.11, 2019.05, 2020.02, 2020.08, 2020.11, 2021.05. The vulnerability could allow redirect users to malicious websites after authentication.	6.1	More Details
CVE-2021-27578	Cross Site Scripting vulnerability in markdown interpreter of Apache Zeppelin allows an attacker to inject malicious scripts. This issue affects Apache Zeppelin Apache Zeppelin versions prior to 0.9.0.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39278	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP-323-JP-CT-T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.	6.1	More Details
CVE-2021-38641	Microsoft Edge for Android Spoofing Vulnerability	6.1	More Details
CVE-2021-38642	Microsoft Edge for iOS Spoofing Vulnerability	6.1	More Details
CVE-2021-38704	Multiple reflected cross-site scripting (XSS) vulnerabilities in ClinicCases 7.3.3 allow unauthenticated attackers to introduce arbitrary JavaScript by crafting a malicious URL. This can result in account takeover via session token theft.	6.1	More Details
CVE-2021-24599	The Email Encoder – Protect Email Addresses WordPress plugin before 2.1.2 has an endpoint that requires no authentication and will render a user supplied value in the HTML response without escaping or sanitizing the data.	6.1	More Details
CVE-2021-40530	The ElGamal implementation in Crypto++ through 8.5 allows plaintext recovery because, during interaction between two cryptographic libraries, a certain dangerous combination of the prime defined by the receiver's public key, the generator defined by the receiver's public key, and the sender's ephemeral exponents can lead to a cross-configuration attack against OpenPGP.	5.9	More Details
CVE-2021-40529	The ElGamal implementation in Botan through 2.18.1, as used in Thunderbird and other products, allows plaintext recovery because, during interaction between two cryptographic libraries, a certain dangerous combination of the prime defined by the receiver's public key, the generator defined by the receiver's public key, and the sender's ephemeral exponents can lead to a cross-configuration attack against OpenPGP.	5.9	More Details
CVE-2021-40528	The ElGamal implementation in Libgcrypt before 1.9.4 allows plaintext recovery because, during interaction between two cryptographic libraries, a certain dangerous combination of the prime defined by the receiver's public key, the generator defined by the receiver's public key, and the sender's ephemeral exponents can lead to a cross-configuration attack against OpenPGP.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32782	Nextcloud Circles is an open source social network built for the nextcloud ecosystem. In affected versions the Nextcloud Circles application is vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. It is recommended that the Nextcloud Circles application is upgraded to 0.21.3, 0.20.10 or 0.19.14 to resolve this issue. As a workaround users may use a browser that has support for Content-Security-Policy. A notable exemption is Internet Explorer which does not support CSP properly.	5.8	More Details
CVE-2021-31611	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication.	5.7	More Details
CVE-2021-36094	It's possible to craft a request for appointment edit screen, which could lead to the XSS attack. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior versions.	5.7	More Details
CVE-2021-23438	This affects the package mpath before 0.8.4. A type confusion vulnerability can lead to a bypass of CVE-2018-16490. In particular, the condition ignoreProperties.indexOf(parts[i]) !== -1 returns -1 if parts[i] is ['__proto__']. This is because the method that has been called if the input is an array is Array.prototype.indexOf() and not String.prototype.indexOf(). They behave differently depending on the type of the input.	5.6	More Details
CVE-2021-23426	This affects all versions of package Proto. It is possible to inject pollute the object property of an application using Proto by leveraging the merge function.	5.6	More Details
CVE-2021-23436	This affects the package immer before 9.0.6. A type confusion vulnerability can lead to a bypass of CVE-2020-28477 when the user-provided keys used in the path parameter are arrays. In particular, this bypass is possible because the condition (p === "__proto__" || p === "constructor") in applyPatches_ returns false if p is ['__proto__'] (or ['constructor']). The === operator (strict equality operator) returns false if the operands have different type.	5.6	More Details
CVE-2021-36077	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SVG file, potentially resulting in local application denial of service in the context of the current user. User interaction is required to exploit this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36056	XMP Toolkit SDK version 2020.1 (and earlier) is affected by a buffer overflow vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file.	5.5	More Details
CVE-2021-39257	A crafted NTFS image with an unallocated bitmap can lead to a endless recursive function call chain (starting from ntfs_attr_pwrite), causing stack consumption in NTFS-3G < 2021.8.22.	5.5	More Details
CVE-2021-34733	A vulnerability in the CLI of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow an authenticated, local attacker to access sensitive information stored on the underlying file system of an affected system. This vulnerability exists because sensitive information is not sufficiently secured when it is stored. An attacker could exploit this vulnerability by gaining unauthorized access to sensitive information on an affected system. A successful exploit could allow the attacker to create forged authentication requests and gain unauthorized access to the affected system.	5.5	More Details
CVE-2021-22525	This release addresses a potential information leakage vulnerability in NetIQ Access Manager versions prior to 5.0.1	5.5	More Details
CVE-2021-36058	XMP Toolkit SDK version 2020.1 (and earlier) is affected by an Integer Overflow vulnerability potentially resulting in application-level denial of service in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file.	5.5	More Details
CVE-2021-32801	Nextcloud server is an open source, self hosted personal cloud. In affected versions logging of exceptions may have resulted in logging potentially sensitive key material for the Nextcloud Encryption-at-Rest functionality. It is recommended that the Nextcloud Server is upgraded to 20.0.12, 21.0.4 or 22.1.0. If upgrading is not an option users are advised to disable system logging to resolve this issue until such time that an upgrade can be performed Note that ff you do not use the Encryption-at-Rest functionality of Nextcloud you are not affected by this bug.	5.5	More Details
CVE-2021-35948	Session fixation on password protected public links in the ownCloud Server before 10.8.0 allows an attacker to bypass the password protection when they can force a target client to use a controlled cookie.	5.4	More Details
CVE-2020-20349	WTCMS 1.0 contains a stored cross-site scripting (XSS) vulnerability in the link address field under the background links module.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36061	Adobe Connect version 11.2.2 (and earlier) is affected by a secure design principles violation vulnerability via the 'pbMode' parameter. An unauthenticated attacker could leverage this vulnerability to edit or delete recordings on the Connect environment. Exploitation of this issue requires user interaction in that a victim must publish a link of a Connect recording.	5.4	More Details
CVE-2021-36062	Adobe Connect version 11.2.2 (and earlier) is affected by a Reflected Cross-site Scripting vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2021-38707	Persistent cross-site scripting (XSS) vulnerabilities in ClinicCases 7.3.3 allow low-privileged attackers to introduce arbitrary JavaScript to account parameters. The XSS payloads will execute in the browser of any user who views the relevant content. This can result in account takeover via session token theft.	5.4	More Details
CVE-2021-36063	Adobe Connect version 11.2.2 (and earlier) is affected by a Reflected Cross-site Scripting vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2021-39496	Eyoucms 1.5.4 lacks sanitization of input data, allowing an attacker to inject malicious code into `filename` param to trigger Reflected XSS.	5.4	More Details
CVE-2021-29852	IBM Planning Analytics 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 205528.	5.4	More Details
CVE-2021-40509	ViewCommon.java in JForum2 2.7.0 allows XSS via a user signature.	5.4	More Details
CVE-2021-33483	An issue was discovered in CommentsService.ashx in OnyakTech Comments Pro 3.8. The comment posting functionality allows an attacker to add an XSS payload to the JSON request that will execute when users visit the page with the comment.	5.4	More Details
CVE-2020-20344	WTCMS 1.0 contains a reflective cross-site scripting (XSS) vulnerability in the keyword search function under the background articles module.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20345	WTCMS 1.0 contains a reflective cross-site scripting (XSS) vulnerability in the page management background which allows attackers to obtain cookies via a crafted payload entered into the search box.	5.4	More Details
CVE-2020-20347	WTCMS 1.0 contains a stored cross-site scripting (XSS) vulnerability in the source field under the article management module.	5.4	More Details
CVE-2020-20348	WTCMS 1.0 contains a stored cross-site scripting (XSS) vulnerability in the link field under the background menu management module.	5.4	More Details
CVE-2021-36696	Deskpro cloud and on-premise Deskpro 2021.1.6 and fixed in Deskpro 2021.1.7 contains a cross-site scripting (XSS) vulnerability in social media links on a user profile due to lack of input validation.	5.4	More Details
CVE-2021-3768	bookstack is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-24601	The WPFront Notification Bar WordPress plugin before 2.1.0.08087 does not properly sanitise and escape its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	5.4	More Details
CVE-2021-24517	The Stop Spammers Security	Block Spam Users, Comments, Forms WordPress plugin before 2021.18 does not escape some of its settings, allowing high privilege users such as admin to set Cross-Site Scripting payloads in them even when the unfiltered_html capability is disallowed	5.4	More Details
CVE-2021-24513	The Form Builder	Create Responsive Contact Forms WordPress plugin before 1.9.8.4 does not sanitise or escape its Form Title, allowing high privilege users such as admin to set Cross-Site Scripting payload in them, even when the unfiltered_html capability is disallowed	5.4	More Details
CVE-2021-24603	The Site Reviews WordPress plugin before 5.13.1 does not sanitise some of its Review Details when adding a review as an admin, which could allow them to perform Cross-Site Scripting attacks when the unfiltered_html is disallowed	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24590	The Cookie Notice & Consent Banner for GDPR & CCPA Compliance WordPress plugin before 1.7.2 does not properly sanitize inputs to prevent injection of arbitrary HTML within the plugin's design customization options.	5.4	More Details
CVE-2021-24611	The Keyword Meta WordPress plugin through 3.0 does not sanitise of escape its settings before outputting them back in the page after they are saved, allowing for Cross-Site Scripting issues. Furthermore, it is also lacking any CSRF check, allowing attacker to make a logged in high privilege user save arbitrary setting via a CSRF attack.	5.4	More Details
CVE-2021-24591	The Highlight WordPress plugin before 0.9.3 does not sanitise its CustomCSS setting, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	5.4	More Details
CVE-2021-24568	The AddToAny Share Buttons WordPress plugin before 1.7.46 does not sanitise its Sharing Header setting when outputting it in frontend pages, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	5.4	More Details
CVE-2021-36717	Synerion TimeNet version 9.21 contains a directory traversal vulnerability where, on the "Name" parameter, the attacker can return to the root directory and open the host file. This might give the attacker the ability to view restricted files, which could provide the attacker with more information required to further compromise the system.	5.4	More Details
CVE-2021-3767	bookstack is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-37151	CyberArk Identity 21.5.131, when handling an invalid authentication attempt, sometimes reveals whether the username is valid. In certain authentication policy configurations with MFA, the API response length can be used to differentiate between a valid user and an invalid one (aka Username Enumeration). Response differentiation enables attackers to enumerate usernames of valid application users. Attackers can use this information to leverage brute-force and dictionary attacks in order to discover valid account information such as passwords.	5.3	More Details
CVE-2021-36095	Malicious attacker is able to find out valid user logins by using the "lost password" feature. This issue affects: OTRS AG ((OTRS)) Community Edition version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior versions.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39119	Affected versions of Atlassian Jira Server and Data Center allow users who have watched an issue to continue receiving updates on the issue even after their Jira account is revoked, via a Broken Access Control vulnerability in the issue notification feature. The affected versions are before version 8.19.0.	5.3	More Details
CVE-2021-35949	The shareinfo controller in the ownCloud Server before 10.8.0 allows an attacker to bypass the permission checks for upload only shares and list metadata about the share.	5.3	More Details
CVE-2021-35947	The public share controller in the ownCloud server before version 10.8.0 allows a remote attacker to see the internal path and the username of a public share by including invalid characters in the URL.	5.3	More Details
CVE-2021-36930	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	5.3	More Details
CVE-2021-28559	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by an Information Exposure vulnerability. An unauthenticated attacker could leverage this vulnerability to get access to restricted data stored within global variables and objects.	5.3	More Details
CVE-2021-32766	Nextcloud Text is an open source plaintext editing application which ships with the nextcloud server. In affected versions the Nextcloud Text application returned different error messages depending on whether a folder existed in a public link share. This is problematic in case the public link share has been created with "Upload Only" privileges. (aka "File Drop"). A link share recipient is not expected to see which folders or files exist in a "File Drop" share. Using this vulnerability an attacker is able to enumerate folders in such a share. Exploitation requires that the attacker has access to a valid affected "File Drop" link share. It is recommended that the Nextcloud Server is upgraded to 20.0.12, 21.0.4 or 22.0.1. Users who are unable to upgrade are advised to disable the Nextcloud Text application in the app settings.	5.3	More Details
CVE-2021-34145	The Bluetooth Classic implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 devices does not properly handle the reception of LMP_max_slot with an invalid Baseband packet type (and LT_ADDRESS and LT_ADDR) after completion of the LMP setup procedure, allowing attackers in radio range to trigger a denial of service (firmware crash) via a crafted LMP packet.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36093	It's possible to create an email which can be stuck while being processed by PostMaster filters, causing DoS. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior versions; 8.0.x version 8.0.15 and prior versions.	5.3	More Details
CVE-2021-37629	Nextcloud Richdocuments is an open source collaborative office suite. In affected versions there is a lack of rate limiting on the Richdocuments OCS endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. It is recommended that the Nextcloud Richdocuments app is upgraded to either 3.8.4 or 4.2.1 to resolve. For users unable to upgrade it is recommended that the Richdocuments application be disabled.	5.3	More Details
CVE-2021-38314	The Gutenberg Template Library & Redux Framework plugin <= 4.2.11 for WordPress registered several AJAX actions available to unauthenticated users in the `includes` function in `redux-core/class-redux-core.php` that were unique to a given site but deterministic and predictable given that they were based on an md5 hash of the site URL with a known salt value of '-redux' and an md5 hash of the previous hash with a known salt value of '-support'. These AJAX actions could be used to retrieve a list of active plugins and their versions, the site's PHP version, and an unsalted md5 hash of site's `AUTH_KEY` concatenated with the `SECURE_AUTH_KEY`.	5.3	More Details
CVE-2021-39193	Frontier is Substrate's Ethereum compatibility layer. Prior to commit number 0b962f218f0cdd796dadfe26c3f09e68f7861b26, a bug in `pallet-ethereum` can cause invalid transactions to be included in the Ethereum block state in `pallet-ethereum` due to not validating the input data size. Any invalid transactions included this way have no possibility to alter the internal Ethereum or Substrate state. The transaction will appear to have be included, but is of no effect as it is rejected by the EVM engine. The impact is further limited by Substrate extrinsic size constraints. A patch is available in commit number 0b962f218f0cdd796dadfe26c3f09e68f7861b26. There are no workarounds aside from applying the patch.	5.3	More Details
CVE-2021-36096	Generated Support Bundles contains private S/MIME and PGP keys if containing folder is not hidden. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior versions; 8.0.x version 8.0.15 and prior versions.	5.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31797	The user identification mechanism used by CyberArk Credential Provider prior to 12.1 is susceptible to a local host race condition, leading to password disclosure.	5.1	More Details
CVE-2021-36002	Adobe Captivate version 11.5.5 (and earlier) is affected by an Creation of Temporary File In Directory With Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. The attacker must plant a malicious file in a particular location of the victim's machine. Exploitation of this issue requires user interaction in that a victim must launch the Captivate Installer.	5.0	More Details
CVE-2021-37733	A remote path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.11, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	4.9	More Details
CVE-2021-27022	A flaw was discovered in bolt-server and ace where running a task with sensitive parameters results in those sensitive parameters being logged when they should not be. This issue only affects SSH/WinRM nodes (inventory service nodes).	4.9	More Details
CVE-2021-34759	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker would need valid administrative credentials.	4.8	More Details
CVE-2021-35238	User with Orion Platform Admin Rights could store XSS through URL POST parameter in CreateExternalWebsite website.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39191	mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9.4, the 3rd-party init SSO functionality of mod_auth_openidc was reported to be vulnerable to an open redirect attack by supplying a crafted URL in the `target_link_uri` parameter. A patch in version 2.4.9.4 made it so that the `OIDCRedirectURLsAllowed` setting must be applied to the `target_link_uri` parameter. There are no known workarounds aside from upgrading to a patched version.	4.7	More Details
CVE-2021-26439	Microsoft Edge for Android Information Disclosure Vulnerability	4.6	More Details
CVE-2021-33599	A vulnerability affecting F-Secure Antivirus engine was discovered whereby scanning WIM archive file can lead to denial-of-service (infinite loop and freezes AV engine scanner). The vulnerability can be exploit remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine.	4.6	More Details
CVE-2021-31798	The effective key space used to encrypt the cache in CyberArk Credential Provider prior to 12.1 has low entropy, and under certain conditions a local malicious user can obtain the plaintext of cache files.	4.4	More Details
CVE-2021-39186	GlobalNewFiles is a MediaWiki extension maintained by Miraheze. Prior to commit number cee254e1b158cdb0ddbea716b1d3edc31fa4fb5d, the username column of the GlobalNewFiles special page is vulnerable to a stored XSS. Commit number cee254e1b158cdb0ddbea716b1d3edc31fa4fb5d contains a patch. As a workaround, one may disallow <,> (or other characters required to insert html/js) from being used in account names so an XSS is not possible.	4.3	More Details
CVE-2021-29853	IBM Planning Analytics 2.0 could expose information that could be used to to create attacks by not validating the return values from some methods or functions. IBM X-Force ID: 205529.	4.3	More Details
CVE-2021-28565	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by an Out-of-bounds Read vulnerability in the PDFLibTool component. 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.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39194	kaml is an open source implementation of the YAML format with support for kotlinx.serialization. In affected versions attackers that could provide arbitrary YAML input to an application that uses kaml could cause the application to endlessly loop while parsing the input. This could result in resource starvation and denial of service. This only affects applications that use polymorphic serialization with the default tagged polymorphism style. Applications using the property polymorphism style are not affected. YAML input for a polymorphic type that provided a tag but no value for the object would trigger the issue. Version 0.35.3 or later contain the fix for this issue.	4.3	More Details
CVE-2021-29851	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information when a stack trace is returned in the browser. IBM X-Force ID: 205527.	4.3	More Details
CVE-2021-34765	A vulnerability in the web UI for Cisco Nexus Insights could allow an authenticated, remote attacker to view and download files related to the web application. The attacker requires valid device credentials. This vulnerability exists because proper role-based access control (RBAC) filters are not applied to file download actions. An attacker could exploit this vulnerability by logging in to the application and then navigating to the directory listing and download functions. A successful exploit could allow the attacker to download sensitive files that should be restricted, which could result in disclosure of sensitive information.	4.3	More Details
CVE-2020-15939	An improper access control vulnerability (CWE-284) in FortiSandbox versions 3.2.1 and below and 3.1.4 and below may allow an authenticated, unprivileged attacker to download the device configuration file via the recovery URL.	4.3	More Details
CVE-2021-28557	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to leak sensitive system information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4.3	More Details
CVE-2021-23439	This affects the package file-upload-with-preview before 4.2.0. A file containing malicious JavaScript code in the name can be uploaded (a user needs to be tricked into uploading such a file).	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35995	Adobe After Effects version 18.2.1 (and earlier) is affected by an Improper input validation vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2021-36018	Adobe After Effects version 18.2.1 (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 disclose sensitive memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2021-36019	Adobe After Effects version 18.2.1 (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 disclose arbitrary memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2021-36074	Adobe Bridge versions 11.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2021-36071	Adobe Bridge versions 11.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2021-36057	XMP Toolkit SDK version 2020.1 (and earlier) is affected by a write-what-where condition vulnerability caused during the application's memory allocation process. This may cause the memory management functions to become mismatched resulting in local application denial of service in the context of the current user.	3.3	More Details
CVE-2021-36054	XMP Toolkit SDK version 2020.1 (and earlier) is affected by a buffer overflow vulnerability potentially resulting in local application denial of service in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36045	XMP Toolkit SDK versions 2020.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2021-36053	XMP Toolkit SDK versions 2020.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2021-25737	A security issue was discovered in Kubernetes where a user may be able to redirect pod traffic to private networks on a Node. Kubernetes already prevents creation of Endpoint IPs in the localhost or link-local range, but the same validation was not performed on EndpointSlice IPs.	2.7	More Details
CVE-2021-28558	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by an Heap-based buffer overflow vulnerability in the PDFLibTool component. 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-2021-28555	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to get access to 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