SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 06 October 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-2020-12030	There is a flaw in the code used to configure the internal gateway firewall when the gateway's VLAN feature is enabled. If a user enables the VLAN setting, the internal gateway firewall becomes disabled resulting in exposure of all ports used by the gateway.	10.0	More Details
CVE-2021-23857	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system.	10.0	More Details
CVE-2021-23856	The web server is vulnerable to reflected XSS and therefore an attacker might be able to execute scripts on a client’s computer by sending the client a manipulated URL.	10.0	More Details
CVE-2021-33924	Confluent Ansible (cp-ansible) version 5.5.0, 5.5.1, 5.5.2 and 6.0.0 is vulnerable to Incorrect Access Control via its auxiliary component that allows remote attackers to access sensitive information.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41511	The username and password field of login in Lodging Reservation Management System V1 can give access to any user by using SQL injection to bypass authentication.	9.8	More Details
CVE-2021-40960	Galera WebTemplate 1.0 is affected by a directory traversal vulnerability that could reveal information from /etc/passwd and /etc/shadow.	9.8	More Details
CVE-2021-41649	An un-authenticated SQL Injection exists in PuneethReddyHC online-shopping-system-advanced through the /homeaction.php cat_id parameter. Using a post request does not sanitize the user input.	9.8	More Details
CVE-2020-21012	Sourcecodester Hotel and Lodge Management System 2.0 is vulnerable to unauthenticated SQL injection and can allow remote attackers to execute arbitrary SQL commands via the email parameter to the edit page for Customer, Room, Currency, Room Booking Details, or Tax Details.	9.8	More Details
CVE-2021-41862	AviatorScript through 5.2.7 allows code execution via an expression that is encoded with Byte Code Engineering Library (BCEL).	9.8	More Details
CVE-2021-40323	Cobbler before 3.3.0 allows log poisoning, and resultant Remote Code Execution, via an XMLRPC method that logs to the logfile for template injection.	9.8	More Details
CVE-2021-38823	The IceHrm 30.0.0 OS website was found vulnerable to Session Management Issue. A signout from an admin account does not invalidate an admin session that is opened in a different browser.	9.8	More Details
CVE-2021-37333	Laravel Booking System Booking Core 2.0 is vulnerable to Session Management. A password change at sandbox.bookingcore.org/user/profile/change-password does not invalidate a session that is opened in a different browser.	9.8	More Details
CVE-2020-20796	FlameCMS 3.3.5 contains a SQL injection vulnerability in /master/article.php via the "Id" parameter.	9.8	More Details
CVE-2021-41868	OnionShare 2.3 before 2.4 allows remote unauthenticated attackers to upload files on a non-public node when using the --receive functionality.	9.8	More Details
CVE-2021-35296	An issue in the administrator authentication panel of PTCL HG150-Ub v3.0 allows attackers to bypass authentication via modification of the cookie value and Response Path.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41553	In ARCHIBUS Web Central 21.3.3.815 (a version from 2014), the Web Application in /archibus/login.axvw assign a session token that could be already in use by another user. It was therefore possible to access the application through a user whose credentials were not known, without any attempt by the testers to modify the application logic. It is also possible to set the value of the session token, client-side, simply by making an unauthenticated GET Request to the Home Page and adding an arbitrary value to the JSESSIONID field. The application, following the login, does not assign a new token, continuing to keep the inserted one, as the identifier of the entire session. This is fixed in all recent versions, such as version 26. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Version 21.3 was officially de-supported by the end of 2020	9.8	More Details
CVE-2021-39226	Grafana is an open source data visualization platform. In affected versions unauthenticated and authenticated users are able to view the snapshot with the lowest database key by accessing the literal paths: /dashboard/snapshot/:key, or /api/snapshots/:key. If the snapshot "public_mode" configuration setting is set to true (vs default of false), unauthenticated users are able to delete the snapshot with the lowest database key by accessing the literal path: /api/snapshots-delete/:deleteKey. Regardless of the snapshot "public_mode" setting, authenticated users are able to delete the snapshot with the lowest database key by accessing the literal paths: /api/snapshots/:key, or /api/snapshots-delete/:deleteKey. The combination of deletion and viewing enables a complete walk through all snapshot data while resulting in complete snapshot data loss. This issue has been resolved in versions 8.1.6 and 7.5.11. If for some reason you cannot upgrade you can use a reverse proxy or similar to block access to the literal paths: /api/snapshots/:key, /api/snapshots-delete/:deleteKey, /dashboard/snapshot/:key, and /api/snapshots/:key. They have no normal function and can be disabled without side effects.	9.8	More Details
CVE-2021-36745	A vulnerability in Trend Micro ServerProtect for Storage 6.0, ServerProtect for EMC Celerra 5.8, ServerProtect for Network Appliance Filers 5.8, and ServerProtect for Microsoft Windows / Novell Netware 5.8 could allow a remote attacker to bypass authentication on affected installations.	9.8	More Details
CVE-2020-20797	FlameCMS 3.3.5 contains a time-based blind SQL injection vulnerability in /account/register.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33583	REINER timeCard 6.05.07 installs a Microsoft SQL Server with an sa password that is hardcoded in the TCServer.jar file.	9.8	More Details
CVE-2021-41616	Apache DB DdlUtils 1.0 included a BinaryObjectsHelper that was intended for use when migrating database data with a SQL data type of BINARY, VARBINARY, LONGVARBINARY, or BLOB between databases using the ddlutils features. The BinaryObjectsHelper class was insecure and used ObjectInputStream.readObject without validating that the input data was safe to deserialize. Please note that DdlUtils is no longer being actively developed. To address the insecurity of the BinaryObjectHelper class, the following changes to DdlUtils have been made: (1) BinaryObjectsHelper.java has been deleted from the DdlUtils source repository and the DdlUtils feature of propagating data of SQL binary types is therefore no longer present in DdlUtils; (2) The ddlutils-1.0 release has been removed from the Apache Release Distribution Infrastructure; (3) The DdlUtils web site has been updated to indicate that DdlUtils is now available only as source code, not as a packaged release.	9.8	More Details
CVE-2021-35943	Couchbase Server 6.5.x and 6.6.x through 6.6.2 has Incorrect Access Control. Externally managed users are not prevented from using an empty password, per RFC4513.	9.8	More Details
CVE-2021-20578	IBM Cloud Pak for Security (CP4S) 1.7.0.0, 1.7.1.0, 1.7.2.0, and 1.8.0.0 could allow an attacker to perform unauthorized actions due to improper or missing authentication controls. IBM X-Force ID: 199282.	9.8	More Details
CVE-2020-18683	Floodlight through 1.2 has poor input validation in checkFlow in StaticFlowEntryPusherResource.java because of undefined fields mishandling.	9.8	More Details
CVE-2020-18684	Floodlight through 1.2 has an integer overflow in checkFlow in StaticFlowEntryPusherResource.java via priority or port number.	9.8	More Details
CVE-2020-18685	Floodlight through 1.2 has poor input validation in checkFlow in StaticFlowEntryPusherResource.java because of unchecked prerequisites related to TCP or UDP ports, or group or table IDs.	9.8	More Details
CVE-2021-41301	ECOA BAS controller is vulnerable to configuration disclosure when direct object reference is made to the specific files using an HTTP GET request. This will enable the unauthenticated attacker to remotely disclose sensitive information and help her in authentication bypass, privilege escalation and full system access.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41300	ECOA BAS controller's special page displays user account and passwords in plain text, thus unauthenticated attackers can access the page and obtain privilege with full functionality.	9.8	More Details
CVE-2021-41299	ECOA BAS controller is vulnerable to hard-coded credentials within its Linux distribution image, thus remote attackers can obtain administrator's privilege without logging in.	9.8	More Details
CVE-2021-41296	ECOA BAS controller uses weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system.	9.8	More Details
CVE-2021-41288	Zoho ManageEngine OpManager version 125466 and below is vulnerable to SQL Injection in the getReportData API.	9.8	More Details
CVE-2021-41292	ECOA BAS controller suffers from an authentication bypass vulnerability. An unauthenticated attacker through cookie poisoning can remotely bypass authentication and disclose sensitive information and circumvent physical access controls in smart homes and buildings and manipulate HVAC.	9.8	More Details
CVE-2021-41290	ECOA BAS controller suffers from an arbitrary file write and path traversal vulnerability. Using the POST parameters, unauthenticated attackers can remotely set arbitrary values for location and content type and gain the possibility to execute arbitrary code on the affected device.	9.8	More Details
CVE-2021-3625	Buffer overflow in Zephyr USB DFU DNLOAD. Zephyr versions >= v2.5.0 contain Heap-based Buffer Overflow (CWE-122). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-c3gr-hgvr-f363	9.6	More Details
CVE-2021-3825	On 2.1.15 version and below of Lider module in LiderAhenk software is leaking it's configurations via an unsecured API. An attacker with an access to the configurations API could get valid LDAP credentials.	9.6	More Details
CVE-2021-41591	ACINQ Eclair before 0.6.3 allows loss of funds because of dust HTLC exposure.	9.4	More Details
CVE-2021-41592	Blockstream c-lightning through 0.10.1 allows loss of funds because of dust HTLC exposure.	9.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41647	An un-authenticated error-based and time-based blind SQL injection vulnerability exists in Kaushik Jadhav Online Food Ordering Web App 1.0. An attacker can exploit the vulnerable "username" parameter in login.php and retrieve sensitive database information, as well as add an administrative user.	9.1	More Details
CVE-2021-41729	BaiCloud-cms v2.5.7 is affected by an arbitrary file deletion vulnerability, which allows an attacker to delete arbitrary files on the server through /user/ppsave.php.	9.1	More Details
CVE-2021-41110	cwlviewer is a web application to view and share Common Workflow Language workflows. Versions prior to 1.3.1 contain a Deserialization of Untrusted Data vulnerability. Commit number f6066f09edb70033a2ce80200e9fa9e70a5c29de (dated 2021-09-30) contains a patch. There are no available workarounds aside from installing the patch. The SnakeYaml constructor, by default, allows any data to be parsed. To fix the issue the object needs to be created with a `SafeConstructor` object, as seen in the patch.	9.1	More Details
CVE-2021-41294	ECOA BAS controller suffers from a path traversal vulnerability, causing arbitrary files deletion. Using the specific GET parameter, unauthenticated attackers can remotely delete arbitrary files on the affected device and cause denial of service scenario.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-3626	The Windows version of Multipass before 1.7.0 allowed any local process to connect to the localhost TCP control socket to perform mounts from the operating system to a guest, allowing for privilege escalation.	8.8	More Details
CVE-2021-3747	The MacOS version of Multipass, version 1.7.0, fixed in 1.7.2, accidentally installed the application directory with incorrect owner.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41113	TYPO3 is an open source PHP based web content management system released under the GNU GPL. It has been discovered that the new TYPO3 v11 feature that allows users to create and share deep links in the backend user interface is vulnerable to cross-site-request-forgery. The impact is the same as described in TYPO3-CORE-SA-2020-006 (CVE-2020-11069). However, it is not limited to the same site context and does not require the attacker to be authenticated. In a worst case scenario, the attacker could create a new admin user account to compromise the system. To successfully carry out an attack, an attacker must trick his victim to access a compromised system. The victim must have an active session in the TYPO3 backend at that time. The following Same-Site cookie settings in $GLOBALS[TYPO3_CONF_VARS][BE][cookieSameSite] are required for an attack to be successful: SameSite=strict: malicious evil.example.org invoking TYPO3 application at good.example.org and SameSite=lax or none: malicious evil.com invoking TYPO3 application at example.org. Update your instance to TYPO3 version 11.5.0 which addresses the problem described.	8.8	More Details
CVE-2021-3653	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "int_ctl" field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. This flaw affects Linux kernel versions prior to 5.14-rc7.	8.8	More Details
CVE-2021-41764	A cross-site request forgery (CSRF) vulnerability exists in Streama up to and including v1.10.3. The application does not have CSRF checks in place when performing actions such as uploading local files. As a result, attackers could make a logged-in administrator upload arbitrary local files via a CSRF attack and send them to the attacker.	8.8	More Details
CVE-2021-41824	Craft CMS before 3.7.14 allows CSV injection.	8.8	More Details
CVE-2021-41295	ECOA BAS controller has a Cross-Site Request Forgery vulnerability, thus authenticated attacker can remotely place a forged request at a malicious web page and execute CRUD commands (GET, POST, PUT, DELETE) to perform arbitrary operations in the system.	8.8	More Details
CVE-2021-41297	ECOA BAS controller is vulnerable to weak access control mechanism allowing authenticated user to remotely escalate privileges by disclosing credentials of administrative accounts in plain-text.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41298	ECOA BAS controller is vulnerable to insecure direct object references that occur when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability, attackers with general user's privilege can remotely bypass authorization and access the hidden resources in the system and execute privileged functionalities.	8.8	More Details
CVE-2021-42006	An out-of-bounds access in GffLine::GffLine in gff.cpp in GCLib 0.12.7 allows an attacker to cause a segmentation fault or possibly have unspecified other impact via a crafted GFF file.	8.8	More Details
CVE-2021-32765	Hiredis is a minimalistic C client library for the Redis database. In affected versions Hiredis is vulnurable to integer overflow if provided maliciously crafted or corrupted `RESP` `mult-bulk` protocol data. When parsing `multi-bulk` (array-like) replies, hiredis fails to check if `count * sizeof(redisReply*)` can be represented in `SIZE_MAX`. If it can not, and the `calloc()` call doesn't itself make this check, it would result in a short allocation and subsequent buffer overflow. Users of hiredis who are unable to update may set the [maxelements] (https://github.com/redis/hiredis#reader-max-array-elements) context option to a value small enough that no overflow is possible.	8.8	More Details
CVE-2020-21386	A Cross-Site Request Forgery (CSRF) in the component admin.php/admin/type/info.html of Maccms 10 allows attackers to gain administrator privileges.	8.8	More Details
CVE-2021-41554	ARCHIBUS Web Central 21.3.3.815 (a version from 2014) does not properly validate requests for access to data and functionality in these affected endpoints: /archibus/schema/ab-edit-users.axvw, /archibus/schema/ab-data-dictionary-table.axvw, /archibus/schema/ab-schema-add-field.axvw, /archibus/schema/ab-core/views/process-navigator/ab-my-user-profile.axvw. By not verifying the permissions for access to resources, it allows a potential attacker to view pages that are not allowed. Specifically, it was found that any authenticated user can reach the administrative console for user management by directly requesting access to the page via URL. This allows a malicious user to modify all users' profiles, to elevate any privileges to administrative ones, or to create or delete any type of user. It is also possible to modify the emails of other users, through a misconfiguration of the username parameter, on the user profile page. This is fixed in all recent versions, such as version 26. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Version 21.3 was officially de-supported by the end of 2020	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23893	Privilege Escalation vulnerability in a Windows system driver of McAfee Drive Encryption (DE) prior to 7.3.0 could allow a local non-admin user to gain elevated system privileges via exploiting an unutilized memory buffer.	8.8	More Details
CVE-2021-29108	There is an privilege escalation vulnerability in organization-specific logins in Esri Portal for ArcGIS versions 10.9 and below that may allow a remote, authenticated attacker who is able to intercept and modify a SAML assertion to impersonate another account (XML Signature Wrapping Attack). In addition patching, Esri also strongly recommends as best practice for SAML assertions to be signed and encrypted.	8.8	More Details
CVE-2021-31988	A user controlled parameter related to SMTP test functionality is not correctly validated making it possible to add the Carriage Return and Line Feed (CRLF) control characters and include arbitrary SMTP headers in the generated test email.	8.8	More Details
CVE-2021-41847	An issue was discovered in 3xLogic Infinias Access Control through 6.7.10708.0, affecting physical security. Users with login credentials assigned to a specific zone can send modified HTTP GET and POST requests, allowing them to view user data such as personal information and Prox card credentials. Also, an authorized user of one zone can send API requests to unlock electronic locks associated with zones they are unauthorized to have access to. They can also create new user logins for zones they were not authorized to access, including the root zone of the software.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41322	Poly VVX 400/410 5.3.1 allows low-privileged users to change the Admin password by modifying a POST parameter to 120 during the password reset process.	8.8	More Details
CVE-2021-41869	SuiteCRM 7.10.x before 7.10.33 and 7.11.x before 7.11.22 is vulnerable to privilege escalation.	8.8	More Details
CVE-2021-39885	A Stored XSS in merge request creation page in all versions of Gitlab EE starting from 13.7 before 14.1.7, all versions starting from 14.2 before 14.2.5, and all versions starting from 14.3 before 14.3.1 allows an attacker to execute arbitrary JavaScript code on the victim's behalf via malicious approval rule names	8.7	More Details
CVE-2021-23858	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource.	8.6	More Details
CVE-2021-23855	The user and password data base is exposed by an unprotected web server resource. Passwords are hashed with a weak hashing algorithm and therefore allow an attacker to determine the password by using rainbow tables.	8.6	More Details
CVE-2021-41593	Lightning Labs lnd before 0.13.3-beta allows loss of funds because of dust HTLC exposure.	8.6	More Details
CVE-2021-41116	Composer is an open source dependency manager for the PHP language. In affected versions windows users running Composer to install untrusted dependencies are subject to command injection and should upgrade their composer version. Other OSs and WSL are not affected. The issue has been resolved in composer versions 1.10.23 and 2.1.9. There are no workarounds for this issue.	8.2	More Details
CVE-2021-35491	A Cross-Site Request Forgery (CSRF) vulnerability in Wowza Streaming Engine through 4.8.11+5 allows a remote attacker to delete a user account via the /enginemanager/server/user/delete.htm userName parameter. The application does not implement a CSRF token for the GET request. This issue was resolved in Wowza Streaming Engine release 4.8.14.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24465	The Meow Gallery WordPress plugin before 4.1.9 does not sanitise, validate or escape the ids attribute of its gallery shortcode (available for users as low as Contributor) before using it in an SQL statement, leading to an authenticated SQL Injection issue. The injection also allows the returned values to be manipulated in a way that could lead to data disclosure and arbitrary objects to be deserialized.	8.1	More Details
CVE-2021-41034	The build of some language stacks of Eclipse Che version 6 includes pulling some binaries from an unsecured HTTP endpoint. As a consequence the builds of such stacks are vulnerable to MITM attacks that allow the replacement of the original binaries with arbitrary ones. The stacks involved are Java 8 (alpine and centos), Android and PHP. The vulnerability is not exploitable at runtime but only when building Che.	8.1	More Details
CVE-2021-36298	Dell EMC InsightIQ, versions prior to 4.1.4, contain risky cryptographic algorithms in the SSH component. A remote unauthenticated attacker could potentially exploit this vulnerability leading to authentication bypass and remote takeover of the InsightIQ. This allows an attacker to take complete control of InsightIQ to affect services provided by SSH; so Dell recommends customers to upgrade at the earliest opportunity.	8.1	More Details
CVE-2021-25962	“Shuup” application in versions 0.4.2 to 2.10.8 is affected by the “Formula Injection” vulnerability. A customer can inject payloads in the name input field in the billing address while buying a product. When a store administrator accesses the reports page to export the data as an Excel file and opens it, the payload gets executed.	8.0	More Details
CVE-2021-25961	In “SuiteCRM” application, v7.1.7 through v7.10.31 and v7.11-beta through v7.11.20 fail to properly invalidate password reset links that is associated with a deleted user id, which makes it possible for account takeover of any newly created user with the same user id.	8.0	More Details
CVE-2021-25960	In “SuiteCRM” application, v7.11.18 through v7.11.19 and v7.10.29 through v7.10.31 are affected by “CSV Injection” vulnerability (Formula Injection). A low privileged attacker can use accounts module to inject payloads in the input fields. When an administrator access accounts module to export the data as a CSV file and opens it, the payload gets executed. This was not fixed properly as part of CVE-2020-15301, allowing the attacker to bypass the security measure.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41286	Omikron MultiCash Desktop 4.00.008.SP5 relies on a client-side authentication mechanism. When a user logs into the application, the validity of the password is checked locally. All communication to the database backend is made via the same technical account. Consequently, an attacker can attach a debugger to the process or create a patch that manipulates the behavior of the login function. When the function always returns the success value (corresponding to a correct password), an attacker can login with any desired account, such as the administrative account of the application.	7.8	More Details
CVE-2021-40715	Adobe Premiere Pro version 15.4 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .exr file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	7.8	More Details
CVE-2021-38110	Word97Import200.dll in Corel WordPerfect 2020 20.0.0.200 is affected by an Out-of-bounds Write vulnerability when parsing a 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 DOC file.	7.8	More Details
CVE-2021-42008	The decode_data function in drivers/net/hamradio/6pack.c in the Linux kernel before 5.13.13 has a slab out-of-bounds write. Input from a process that has the CAP_NET_ADMIN capability can lead to root access.	7.8	More Details
CVE-2021-41579	LCDS LAquis SCADA through 4.3.1.1085 is vulnerable to a control bypass and path traversal. If an attacker can get a victim to load a malicious els project file and use the play feature, then the attacker can bypass a consent popup and write arbitrary files to OS locations where the user has permission, leading to code execution.	7.8	More Details
CVE-2021-38101	CDRRip.dll in Corel PhotoPaint Standard 2020 22.0.0.474 is affected by an Out-of-bounds Write vulnerability when parsing a 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 CPT file. This is different from CVE-2021-38099.	7.8	More Details
CVE-2021-38100	Corel PhotoPaint Standard 2020 22.0.0.474 is affected by an Out-of-bounds Write vulnerability when parsing a 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 CPT file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38098	Corel PDF Fusion 2.6.2.0 is affected by a Heap Corruption vulnerability when parsing a 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 PDF file.	7.8	More Details
CVE-2021-38103	IBJPG2.FLT in Corel Presentations 2020 20.0.0.200 is affected by an Out-of-bounds Write vulnerability when parsing a 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 PPT file.	7.8	More Details
CVE-2021-38099	CDRRip.dll in Corel PhotoPaint Standard 2020 22.0.0.474 is affected by an Out-of-bounds Write vulnerability when parsing a 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 CPT file. This is different from CVE-2021-38101.	7.8	More Details
CVE-2021-38096	Coreip.dll in Corel PDF Fusion 2.6.2.0 is affected by an Out-of-bounds Write vulnerability when parsing a 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 PDF file.	7.8	More Details
CVE-2021-38097	Corel PDF Fusion 2.6.2.0 is affected by an Out-of-bounds Write vulnerability when parsing a 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 PDF file.	7.8	More Details
CVE-2021-35297	Scalabium dBase Viewer version 2.6 (Build 5.751) is vulnerable to remote code execution via a crafted DBF file that triggers a buffer overflow. An attacker can use the Structured Exception Handler (SEH) records and redirect execution to attacker-controlled code.	7.8	More Details
CVE-2021-39836	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability in the processing of the AcroForm buttonGetIcon action 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-2021-33626	A vulnerability exists in SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer(QWORD values for CommBuffer). This can be used by an attacker to corrupt data in SMRAM memory and even lead to arbitrary code execution.	7.8	More Details
CVE-2021-39831	Adobe Framemaker versions 2019 Update 8 (and earlier) and 2020 Release Update 2 (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 PDF file.	7.8	More Details
CVE-2021-41864	prealloc_elems_and_freelist in kernel/bpf/stackmap.c in the Linux kernel before 5.14.12 allows unprivileged users to trigger an eBPF multiplication integer overflow with a resultant out-of-bounds write.	7.8	More Details
CVE-2021-41578	mySCADA myDESIGNER 8.20.0 and below allows Directory Traversal attacks when importing project files. If an attacker can trick a victim into importing a malicious mep file, then they gain the ability to write arbitrary files to OS locations where the user has permission. This would typically lead to code execution.	7.8	More Details
CVE-2021-41103	containerd is an open source container runtime with an emphasis on simplicity, robustness and portability. A bug was found in containerd where container root directories and some plugins had insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as setuid), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged Linux user on the host could discover, read, and modify those files. This vulnerability has been fixed in containerd 1.4.11 and containerd 1.5.7. Users should update to these version when they are released and may restart containers or update directory permissions to mitigate the vulnerability. Users unable to update should limit access to the host to trusted users. Update directory permission on container bundles directories.	7.8	More Details
CVE-2021-39843	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (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-2021-41285	Ballistix MOD Utility through 2.0.2.5 is vulnerable to privilege escalation in the MODAPI.sys driver component. The vulnerability is triggered by sending a specific IOCTL request that allows low-privileged users to directly interact with physical memory via the MmMapIoSpace function call (mapping physical memory into a virtual address space). Attackers could exploit this issue to achieve local privilege escalation to NT AUTHORITY\SYSTEM.	7.8	More Details
CVE-2021-39863	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted PDF 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-2021-40683	In Akamai EAA (Enterprise Application Access) Client before 2.3.1, 2.4.x before 2.4.1, and 2.5.x before 2.5.3, an unquoted path may allow an attacker to hijack the flow of execution.	7.8	More Details
CVE-2021-36051	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 specially-crafted .cpp file.	7.8	More Details
CVE-2021-39877	A vulnerability was discovered in GitLab starting with version 12.2 that allows an attacker to cause uncontrolled resource consumption with a specially crafted file.	7.7	More Details
CVE-2021-34356	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Photo Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Photo Station: Photo Station 6.0.18 (2021/09/01) and later	7.6	More Details
CVE-2021-34354	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Photo Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Photo Station: Photo Station 6.0.18 (2021/09/01) and later	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34355	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP NAS running Photo Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Photo Station: Photo Station 5.4.10 (2021/08/19) and later Photo Station 5.7.13 (2021/08/19) and later Photo Station 6.0.18 (2021/09/01) and later	7.6	More Details
CVE-2021-41457	There is a stack buffer overflow in MP4Box 1.1.0 at src/filters/dmx_nhml.c in nhmldmx_init_parsing which leads to a denial of service vulnerability.	7.5	More Details
CVE-2021-41456	There is a stack buffer overflow in MP4Box v1.0.1 at src/filters/dmx_nhml.c:1004 in the nhmldmx_send_sample() function szXmlTo parameter which leads to a denial of service vulnerability.	7.5	More Details
CVE-2021-40324	Cobbler before 3.3.0 allows arbitrary file write operations via upload_log_data.	7.5	More Details
CVE-2021-41530	Forcepoint NGFW Engine versions 6.5.11 and earlier, 6.8.6 and earlier, and 6.10.0 are vulnerable to TCP reflected amplification vulnerability, if HTTP User Response has been configured.	7.5	More Details
CVE-2021-29894	IBM Cloud Pak for Security (CP4S) 1.7.0.0, 1.7.1.0, 1.7.2.0, and 1.8.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 207320.	7.5	More Details
CVE-2020-20665	rudp v0.6 was discovered to contain a memory leak in the component main.c.	7.5	More Details
CVE-2021-41459	There is a stack buffer overflow in MP4Box v1.0.1 at src/filters/dmx_nhml.c:1008 in the nhmldmx_send_sample() function szXmlFrom parameter which leads to a denial of service vulnerability.	7.5	More Details
CVE-2021-31987	A user controlled parameter related to SMTP test functionality is not correctly validated making it possible to bypass blocked network recipients.	7.5	More Details
CVE-2021-41648	An un-authenticated SQL Injection exists in PuneethReddyHC online-shopping-system-advanced through the /action.php prId parameter. Using a post request does not sanitize the user input.	7.5	More Details
CVE-2021-40325	Cobbler before 3.3.0 allows authorization bypass for modification of settings.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41651	A blind SQL injection vulnerability exists in the Raymart DG / Ahmed Helal Hotel-mgmt-system. A malicious attacker can retrieve sensitive database information and interact with the database using the vulnerable cid parameter in process_update_profile.php.	7.5	More Details
CVE-2021-35027	A directory traversal vulnerability in the web server of the Zyxel VPN2S firmware version 1.12 could allow a remote attacker to gain access to sensitive information.	7.5	More Details
CVE-2021-37777	Gila CMS 2.2.0 is vulnerable to Insecure Direct Object Reference (IDOR). Thumbnails uploaded by one site owner are visible by another site owner just by knowing the other site name and fuzzing for picture names. This leads to sensitive information disclosure.	7.5	More Details
CVE-2021-32626	Redis is an open source, in-memory database that persists on disk. In affected versions specially crafted Lua scripts executing in Redis can cause the heap-based Lua stack to be overflowed, due to incomplete checks for this condition. This can result with heap corruption and potentially remote code execution. This problem exists in all versions of Redis with Lua scripting support, starting from 2.6. The problem is fixed in versions 6.2.6, 6.0.16 and 5.0.14. For users unable to update an additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands.	7.5	More Details
CVE-2021-32627	Redis is an open source, in-memory database that persists on disk. In affected versions an integer overflow bug in Redis can be exploited to corrupt the heap and potentially result with remote code execution. The vulnerability involves changing the default proto-max-bulk-len and client-query-buffer-limit configuration parameters to very large values and constructing specially crafted very large stream elements. The problem is fixed in Redis 6.2.6, 6.0.16 and 5.0.14. For users unable to upgrade an additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the proto-max-bulk-len configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32628	Redis is an open source, in-memory database that persists on disk. An integer overflow bug in the ziplist data structure used by all versions of Redis can be exploited to corrupt the heap and potentially result with remote code execution. The vulnerability involves modifying the default ziplist configuration parameters (hash-max-ziplist-entries, hash-max-ziplist-value, zset-max-ziplist-entries or zset-max-ziplist-value) to a very large value, and then constructing specially crafted commands to create very large ziplists. The problem is fixed in Redis versions 6.2.6, 6.0.16, 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the above configuration parameters. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	7.5	More Details
CVE-2021-32675	Redis is an open source, in-memory database that persists on disk. When parsing an incoming Redis Standard Protocol (RESP) request, Redis allocates memory according to user-specified values which determine the number of elements (in the multi-bulk header) and size of each element (in the bulk header). An attacker delivering specially crafted requests over multiple connections can cause the server to allocate significant amount of memory. Because the same parsing mechanism is used to handle authentication requests, this vulnerability can also be exploited by unauthenticated users. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate this problem without patching the redis-server executable is to block access to prevent unauthenticated users from connecting to Redis. This can be done in different ways: Using network access control tools like firewalls, iptables, security groups, etc. or Enabling TLS and requiring users to authenticate using client side certificates.	7.5	More Details
CVE-2021-32687	Redis is an open source, in-memory database that persists on disk. An integer overflow bug affecting all versions of Redis can be exploited to corrupt the heap and potentially be used to leak arbitrary contents of the heap or trigger remote code execution. The vulnerability involves changing the default set-max-intset-entries configuration parameter to a very large value and constructing specially crafted commands to manipulate sets. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the set-max-intset-entries configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32762	Redis is an open source, in-memory database that persists on disk. The redis-cli command line tool and redis-sentinel service may be vulnerable to integer overflow when parsing specially crafted large multi-bulk network replies. This is a result of a vulnerability in the underlying hiredis library which does not perform an overflow check before calling the calloc() heap allocation function. This issue only impacts systems with heap allocators that do not perform their own overflow checks. Most modern systems do and are therefore not likely to be affected. Furthermore, by default redis-sentinel uses the jemalloc allocator which is also not vulnerable. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14.	7.5	More Details
CVE-2021-41099	Redis is an open source, in-memory database that persists on disk. An integer overflow bug in the underlying string library can be used to corrupt the heap and potentially result with denial of service or remote code execution. The vulnerability involves changing the default proto-max-bulk-len configuration parameter to a very large value and constructing specially crafted network payloads or commands. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the proto-max-bulk-len configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	7.5	More Details
CVE-2021-41109	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to version 4.10.4, for regular (non-LiveQuery) queries, the session token is removed from the response, but for LiveQuery payloads it is currently not. If a user has a LiveQuery subscription on the `Parse.User` class, all session tokens created during user sign-ups will be broadcast as part of the LiveQuery payload. A patch in version 4.10.4 removes session tokens from the LiveQuery payload. As a workaround, set `user.acl(new Parse.ACL())` in a beforeSave trigger to make the user private already on sign-up.	7.5	More Details
CVE-2021-39433	A local file inclusion (LFI) vulnerability exists in version BIQS IT Biqs-drive v1.83 and below when sending a specific payload as the file parameter to download/index.php. This allows the attacker to read arbitrary files from the server with the permissions of the configured web-user.	7.5	More Details
CVE-2021-41524	While fuzzing the 2.4.49 httpd, a new null pointer dereference was detected during HTTP/2 request processing, allowing an external source to DoS the server. This requires a specially crafted request. The vulnerability was recently introduced in version 2.4.49. No exploit is known to the project.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41293	ECOA BAS controller suffers from a path traversal vulnerability, causing arbitrary files disclosure. Using the specific POST parameter, unauthenticated attackers can remotely disclose arbitrary files on the affected device and disclose sensitive and system information.	7.5	More Details
CVE-2021-3510	Zephyr JSON decoder incorrectly decodes array of array. Zephyr versions >= >1.14.0, >= >2.5.0 contain Attempt to Access Child of a Non-structure Pointer (CWE-588). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-289f-7mw3-2qf4	7.5	More Details
CVE-2021-35945	Couchbase Server 6.5.x, 6.6.0 through 6.6.2, and 7.0.0, has a Buffer Overflow. A specially crafted network packet sent from an attacker can crash memcached.	7.5	More Details
CVE-2021-35944	Couchbase Server 6.5.x, 6.6.x through 6.6.2, and 7.0.0 has a Buffer Overflow. A specially crafted network packet sent from an attacker can crash memcached.	7.5	More Details
CVE-2021-41773	A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete, see CVE-2021-42013.	7.5	More Details
CVE-2021-22946	A user can tell curl >= 7.20.0 and <= 7.78.0 to require a successful upgrade to TLS when speaking to an IMAP, POP3 or FTP server (`--ssl-reqd` on the command line or`CURLOPT_USE_SSL` set to `CURLUSESSL_CONTROL` or `CURLUSESSL_ALL` withlibcurl). This requirement could be bypassed if the server would return a properly crafted but perfectly legitimate response.This flaw would then make curl silently continue its operations **withoutTLS** contrary to the instructions and expectations, exposing possibly sensitive data in clear text over the network.	7.5	More Details
CVE-2021-41732	An issue was discovered in zeek version 4.1.0. There is a HTTP request splitting vulnerability that will invalidate any ZEEK HTTP based security analysis. NOTE: the vendor's position is that the observed behavior is intended	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41827	Zoho ManageEngine Remote Access Plus before 10.1.2121.1 has hardcoded credentials for read-only access. The credentials are in the source code that corresponds to the DCBackupRestore JAR archive.	7.5	More Details
CVE-2021-41573	Hitachi Content Platform Anywhere (HCP-AW) 4.4.5 and later allows information disclosure. If authenticated user creates a link to a file or folder while the system was running version 4.3.x or earlier and then shares the link and then later deletes the file or folder without deleting the link and before the link expires. If the system has been upgraded to version 4.4.5 or 4.5.0 a malicious user with the link could browse and download all files of the authenticated user that created the link .	7.5	More Details
CVE-2021-23446	The package handsontable before 10.0.0; the package handsontable from 0 and before 10.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) in Handsontable.helper.isNumeric function.	7.5	More Details
CVE-2021-41828	Zoho ManageEngine Remote Access Plus before 10.1.2121.1 has hardcoded credentials associated with resetPWD.xml.	7.5	More Details
CVE-2021-41291	ECOA BAS controller suffers from a path traversal content disclosure vulnerability. Using the GET parameter in File Manager, unauthenticated attackers can remotely disclose directory content on the affected device.	7.5	More Details
CVE-2021-41829	Zoho ManageEngine Remote Access Plus before 10.1.2121.1 relies on the application's build number to calculate a certain encryption key.	7.5	More Details
CVE-2020-20128	LaraCMS v1.0.1 transmits sensitive information in cleartext which can be intercepted by attackers.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35497	The FTL Server (tibftlserver) and Docker images containing tibftlserver components of TIBCO Software Inc.'s TIBCO ActiveSpaces - Community Edition, TIBCO ActiveSpaces - Developer Edition, TIBCO ActiveSpaces - Enterprise Edition, TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, and TIBCO eFTL - Enterprise Edition contain a vulnerability that theoretically allows a non-administrative, authenticated FTL user to trick the affected components into creating illegitimate certificates. These maliciously generated certificates can be used to enable man-in-the-middle attacks or to escalate privileges so that the malicious user has administrative privileges. Affected releases are TIBCO Software Inc.'s TIBCO ActiveSpaces - Community Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO ActiveSpaces - Developer Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO ActiveSpaces - Enterprise Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO FTL - Community Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO FTL - Developer Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO FTL - Enterprise Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO eFTL - Community Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO eFTL - Developer Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, and TIBCO eFTL - Enterprise Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0.	7.5	More Details
CVE-2020-21503	waimai Super Cms 20150505 has a logic flaw allowing attackers to modify a price, before form submission, by observing data in a packet capture. By setting the index.php?m=gift&a=addsave credit parameter to -1, the product is sold for free.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41120	sylius/paypal-plugin is a paypal plugin for the Sylius development platform. In affected versions the URL to the payment page done after checkout was created with autoincremented payment id (/pay-with-paypal/{id}) and therefore it was easy to predict. The problem is that the Credit card form has prefilled "credit card holder" field with the Customer's first and last name and hence this can lead to personally identifiable information exposure. Additionally, the mentioned form did not require authentication. The problem has been patched in Sylius/PayPalPlugin 1.2.4 and 1.3.1. If users are unable to update they can override a sylius_paypal_plugin_pay_with_paypal_form route and change its URL parameters to (for example) {orderToken}/{paymentId}, then override the Sylius\PayPalPlugin\Controller\PayWithPayPalFormAction service, to operate on the payment taken from the repository by these 2 values. It would also require usage of custom repository method. Additionally, one could override the @SyliusPayPalPlugin/payWithPaypal.html.twig template, to add contingencies: ['SCA_ALWAYS'] line in hostedFields.submit(...) function call (line 421). It would then have to be handled in the function callback.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41100	Wire-server is the backing server for the open source wire secure messaging application. In affected versions it is possible to trigger email address change of a user with only the short-lived session token in the `Authorization` header. As the short-lived token is only meant as means of authentication by the client for less critical requests to the backend, the ability to change the email address with a short-lived token constitutes a privilege escalation attack. Since the attacker can change the password after setting the email address to one that they control, changing the email address can result in an account takeover by the attacker. Short-lived tokens can be requested from the backend by Wire clients using the long lived tokens, after which the long lived tokens can be stored securely, for example on the devices key chain. The short lived tokens can then be used to authenticate the client towards the backend for frequently performed actions such as sending and receiving messages. While short-lived tokens should not be available to an attacker per-se, they are used more often and in the shape of an HTTP header, increasing the risk of exposure to an attacker relative to the long-lived tokens, which are stored and transmitted in cookies. If you are running an on-prem instance and provision all users with SCIM, you are not affected by this issue (changing email is blocked for SCIM users). SAML single-sign-on is unaffected by this issue, and behaves identically before and after this update. The reason is that the email address used as SAML NameID is stored in a different location in the databse from the one used to contact the user outside wire. Version 2021-08-16 and later provide a new end-point that requires both the long-lived client cookie and `Authorization` header. The old end-point has been removed. If you are running an on-prem instance with at least some of the users invited or provisioned via SAML SSO and you cannot update then you can block `/self/email` on nginz (or in any other proxies or firewalls you may have set up). You don't need to discriminate by verb: `/self/email` only accepts `PUT` and `DELETE`, and `DELETE` is almost never used.	7.4	More Details
CVE-2021-41093	Wire is an open source secure messenger. In affected versions if the an attacker gets an old but valid access token they can take over an account by changing the email. This issue has been resolved in version 3.86 which uses a new endpoint which additionally requires an authentication cookie. See wire-ios-sync-engine and wire-ios-transport references. This is the root advisory that pulls the changes together.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41124	Scrapy-splash is a library which provides Scrapy and JavaScript integration. In affected versions users who use [`HttpAuthMiddleware`] (http://doc.scrapy.org/en/latest/topics/downloader-middleware.html#module-scrapy.downloadermiddlewares.httpauth) (i.e. the `http_user` and `http_pass` spider attributes) for Splash authentication will have any non-Splash request expose your credentials to the request target. This includes `robots.txt` requests sent by Scrapy when the `ROBOTSTXT_OBEY` setting is set to `True`. Upgrade to scrapy-splash 0.8.0 and use the new `SPLASH_USER` and `SPLASH_PASS` settings instead to set your Splash authentication credentials safely. If you cannot upgrade, set your Splash request credentials on a per-request basis, [using the `splash_headers` request parameter] (https://github.com/scrapy-plugins/scrapy-splash/tree/0.8.x#http-basic-auth), instead of defining them globally using the [`HttpAuthMiddleware`] (http://doc.scrapy.org/en/latest/topics/downloader-middleware.html#module-scrapy.downloadermiddlewares.httpauth). Alternatively, make sure all your requests go through Splash. That includes disabling the [robots.txt middleware] (https://docs.scrapy.org/en/latest/topics/downloader-middleware.html#topics-dlmw-robots).	7.4	More Details
CVE-2021-38618	In GFOS Workforce Management 4.8.272.1, the login page of application is prone to authentication bypass, allowing anyone (who knows a user's credentials except the password) to get access to an account. This occurs because of JSESSIONID mismanagement.	7.4	More Details
CVE-2021-41302	ECOA BAS controller stores sensitive data (backup exports) in clear-text, thus the unauthenticated attacker can remotely query user password and obtain user’s privilege.	7.3	More Details
CVE-2021-35028	A command injection vulnerability in the CGI program of the Zyxel VPN2S firmware version 1.12 could allow an authenticated, local user to execute arbitrary OS commands.	7.3	More Details
CVE-2021-35982	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by an Uncontrolled Search Path Element vulnerability. A local attacker with non-administrative privileges can plant a malicious DLL to achieve arbitrary code execution in the context of the current user via DLL hijacking. Exploitation of this issue requires user interaction.	7.3	More Details
CVE-2021-39887	A stored Cross-Site Scripting vulnerability in the GitLab Flavored Markdown in GitLab CE/EE version 8.4 and above allowed an attacker to execute arbitrary JavaScript code on the victim's behalf.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22261	A stored Cross-Site Scripting vulnerability in the Jira integration in all GitLab versions starting from 13.9 before 14.0.9, all versions starting from 14.1 before 14.1.4, and all versions starting from 14.2 before 14.2.2 allows an attacker to execute arbitrary JavaScript code on the victim's behalf via malicious Jira API responses	7.3	More Details
CVE-2021-40708	Adobe Genuine Service versions 7.3 (and earlier) are affected by a privilege escalation vulnerability in the AGSService installer. An authenticated attacker could leverage this vulnerability to achieve read / write privileges to execute arbitrary code. User interaction is required to abuse this vulnerability.	7.3	More Details
CVE-2020-20746	A stack-based buffer overflow in the httpd server on Tenda AC9 V15.03.06.60_EN allows remote attackers to execute arbitrary code or cause a denial of service (DoS) via a crafted POST request to /goform/SetStaticRouteCfg.	7.2	More Details
CVE-2020-21013	emlog v6.0.0 contains a SQL injection via /admin/comment.php.	7.2	More Details
CVE-2021-35505	Afian FileRun 2021.03.26 allows Remote Code Execution (by administrators) via the Check Path value for the magick binary.	7.2	More Details
CVE-2021-35504	Afian FileRun 2021.03.26 allows Remote Code Execution (by administrators) via the Check Path value for the ffmpeg binary.	7.2	More Details
CVE-2021-34352	A command injection vulnerability has been reported to affect QNAP device running QVR. If exploited, this vulnerability could allow remote attackers to run arbitrary commands. We have already fixed this vulnerability in the following versions of QVR: QVR 5.1.5 build 20210902 and later	7.2	More Details
CVE-2021-36309	Dell Enterprise SONiC OS, versions 3.3.0 and earlier, contains a sensitive information disclosure vulnerability. An authenticated malicious user with access to the system may use the TACACS\Radius credentials stored to read sensitive information and use it in further attacks.	7.1	More Details
CVE-2021-3581	Buffer Access with Incorrect Length Value in zephyr. Zephyr versions >= >=2.5.0 contain Buffer Access with Incorrect Length Value (CWE-805). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-8q65-5gqf-fmw5	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32466	An uncontrolled search path element privilege escalation vulnerability in Trend Micro HouseCall for Home Networks version 5.3.1225 and below could allow an attacker to escalate privileges by placing a custom crafted file in a specific directory to load a malicious library. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	7.0	More Details
CVE-2021-38400	An attacker with physical access to Boston Scientific Zoom Latitude Model 3120 can remove the hard disk drive or create a specially crafted USB to extract the password hash for brute force reverse engineering of the system password.	6.9	More Details
CVE-2021-31986	User controlled parameters related to SMTP notifications are not correctly validated. This can lead to a buffer overflow resulting in crashes and data leakage.	6.8	More Details
CVE-2021-22264	An issue has been discovered in GitLab affecting all versions starting from 13.8 before 14.0.9, all versions starting from 14.1 before 14.1.4, all versions starting from 14.2 before 14.2.2. Under specialized conditions, an invited group member may continue to have access to a project even after the invited group, which the member was part of, is deleted.	6.8	More Details
CVE-2020-21014	emlog v6.0.0 contains an arbitrary file deletion vulnerability in admin/plugin.php.	6.5	More Details
CVE-2021-41795	The Safari app extension bundled with 1Password for Mac 7.7.0 through 7.8.x before 7.8.7 is vulnerable to authorization bypass. By targeting a vulnerable component of this extension, a malicious web page could read a subset of 1Password vault items that would normally be fillable by the user on that web page. These items are usernames and passwords for vault items associated with its domain, usernames and passwords without a domain association, credit cards, and contact items. (1Password must be unlocked for these items to be accessible, but no further user interaction is required.)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35492	Wowza Streaming Engine through 4.8.11+5 could allow an authenticated, remote attacker to exhaust filesystem resources via the /enginemanager/server/vhost/historical.jsdata vhost parameter. This is due to the insufficient management of available filesystem resources. An attacker could exploit this vulnerability through the Virtual Host Monitoring section by requesting random virtual-host historical data and exhausting available filesystem resources. A successful exploit could allow the attacker to cause database errors and cause the device to become unresponsive to web-based management. (Manual intervention is required to free filesystem resources and return the application to an operational state.)	6.5	More Details
CVE-2021-3319	DOS: Incorrect 802154 Frame Validation for Omitted Source / Dest Addresses. Zephyr versions >= > v2.4.0 contain NULL Pointer Dereference (CWE-476), Attempt to Access Child of a Non-structure Pointer (CWE-588). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-94jg-2p6q-5364	6.5	More Details
CVE-2021-39867	In all versions of GitLab CE/EE since version 8.15, a DNS rebinding vulnerability in Gitea Importer may be exploited by an attacker to trigger Server Side Request Forgery (SSRF) attacks.	6.5	More Details
CVE-2021-41845	A SQL injection issue was discovered in ThycoticCentrify Secret Server before 11.0.000007. The only affected versions are 10.9.000032 through 11.0.000006.	6.5	More Details
CVE-2021-39856	Acrobat Reader DC ActiveX Control versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must visit an attacker controlled web page.	6.5	More Details
CVE-2021-39869	In all versions of GitLab CE/EE since version 8.9, project exports may expose trigger tokens configured on that project.	6.5	More Details
CVE-2021-38398	The affected device uses off-the-shelf software components that contain unpatched vulnerabilities. A malicious attacker with physical access to the affected device could exploit these vulnerabilities.	6.5	More Details
CVE-2021-38396	The programmer installation utility does not perform a cryptographic authenticity or integrity checks of the software on the flash drive. An attacker could leverage this weakness to install unauthorized software using a specially crafted USB.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37223	Nagios Enterprises NagiosXI <= 5.8.4 contains a Server-Side Request Forgery (SSRF) vulnerability in schedulereport.php. Any authenticated user can create scheduled reports containing PDF screenshots of any view in the NagiosXI application. Due to lack of input sanitisation, the target page can be replaced with an SSRF payload to access internal resources or disclose local system files.	6.5	More Details
CVE-2021-39880	A Denial Of Service vulnerability in the apollo_upload_server Ruby gem in GitLab CE/EE all versions starting from 11.9 before 14.0.9, all versions starting from 14.1 before 14.1.4, and all versions starting from 14.2 before 14.2.2 allows an attacker to deny access to all users via specially crafted requests to the apollo_upload_server middleware.	6.5	More Details
CVE-2021-40651	OS4Ed OpenSIS Community 8.0 is vulnerable to a local file inclusion vulnerability in Modules.php (modname parameter), which can disclose arbitrary file from the server's filesystem as long as the application has access to the file.	6.5	More Details
CVE-2021-38392	A skilled attacker with physical access to the affected device can gain access to the hard disk drive of the device to change the telemetry region and could use this setting to interrogate or program an implantable device in any region in the world.	6.5	More Details
CVE-2021-39855	Acrobat Reader DC ActiveX Control versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page.	6.5	More Details
CVE-2021-39872	In all versions of GitLab CE/EE since version 14.1, an improper access control vulnerability allows users with expired password to still access GitLab through git and API through access tokens acquired before password expiration.	6.5	More Details
CVE-2021-3709	Function check_attachment_for_errors() in file data/general-hooks/ubuntu.py could be tricked into exposing private data via a constructed crash file. This issue affects: apport 2.14.1 versions prior to 2.14.1-0ubuntu3.29+esm8; 2.20.1 versions prior to 2.20.1-0ubuntu2.30+esm2; 2.20.9 versions prior to 2.20.9-0ubuntu7.26; 2.20.11 versions prior to 2.20.11-0ubuntu27.20; 2.20.11 versions prior to 2.20.11-0ubuntu65.3;	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20663	libiec_iccp_mod v1.5 contains a heap-buffer-overflow in the component mms_client_connection.c.	6.5	More Details
CVE-2020-20662	libiec_iccp_mod v1.5 contains a heap-buffer-overflow in the component mms_client_example1.c.	6.5	More Details
CVE-2020-21431	HongCMS v3.0 contains an arbitrary file read and write vulnerability in the component /admin/index.php/template/edit.	6.5	More Details
CVE-2021-41323	Directory traversal in the Compress feature in Pydio Cells 2.2.9 allows remote authenticated users to overwrite personal files, or Cells files belonging to any user, via the format parameter.	6.5	More Details
CVE-2021-41325	Broken access control for user creation in Pydio Cells 2.2.9 allows remote anonymous users to create standard users via the profile parameter. (In addition, such users can be granted several admin permissions via the Roles parameter.)	6.5	More Details
CVE-2020-20664	libiec_iccp_mod v1.5 contains a segmentation violation in the component server_example1.c.	6.5	More Details
CVE-2021-35201	NEI in NETSCOUT nGeniusONE 6.3.0 build 1196 allows XML External Entity (XXE) attacks.	6.5	More Details
CVE-2021-41821	Wazuh Manager in Wazuh through 4.1.5 is affected by a remote Integer Underflow vulnerability that might lead to denial of service. A crafted message must be sent from an authenticated agent to the manager.	6.5	More Details
CVE-2021-41324	Directory traversal in the Copy, Move, and Delete features in Pydio Cells 2.2.9 allows remote authenticated users to enumerate personal files (or Cells files belonging to any user) via the nodes parameter (for Copy and Move) or via the Path parameter (for Delete).	6.5	More Details
CVE-2021-3710	An information disclosure via path traversal was discovered in apport/hookutils.py function read_file(). This issue affects: apport 2.14.1 versions prior to 2.14.1-0ubuntu3.29+esm8; 2.20.1 versions prior to 2.20.1-0ubuntu2.30+esm2; 2.20.9 versions prior to 2.20.9-0ubuntu7.26; 2.20.11 versions prior to 2.20.11-0ubuntu27.20; 2.20.11 versions prior to 2.20.11-0ubuntu65.3;	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41091	Moby is an open-source project created by Docker to enable software containerization. A bug was found in Moby (Docker Engine) where the data directory (typically `/var/lib/docker`) contained subdirectories with insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as `setuid`), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged Linux user on the host could discover, read, and modify those files. This bug has been fixed in Moby (Docker Engine) 20.10.9. Users should update to this version as soon as possible. Running containers should be stopped and restarted for the permissions to be fixed. For users unable to upgrade limit access to the host to trusted users. Limit access to host volumes to trusted containers.	6.3	More Details
CVE-2021-38394	An attacker with physical access to the device can extract the binary that checks for the hardware key and reverse engineer it, which could be used to create a physical duplicate of a valid hardware key. The hardware key allows access to special settings when inserted.	6.2	More Details
CVE-2021-25959	In OpenCRX, versions v4.0.0 through v5.1.0 are vulnerable to reflected Cross-site Scripting (XSS), due to unsanitized parameters in the password reset functionality. This allows execution of external javascript files on any user of the openCRX instance.	6.1	More Details
CVE-2021-35506	Afian FileRun 2021.03.26 allows XSS when an administrator encounters a crafted document during use of the HTML Editor for a preview or edit action.	6.1	More Details
CVE-2020-21387	A cross-site scripting (XSS) vulnerability in the parameter type_en of Maccms 10 allows attackers to obtain the administrator cookie and escalate privileges via a crafted payload.	6.1	More Details
CVE-2020-21494	A cross-site scripting (XSS) vulnerability in the component install\install.sql of Xiuno BBS 4.0.4 allows attackers to execute arbitrary web scripts or HTML via changing the doctype value to 0.	6.1	More Details
CVE-2021-40973	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the lastname parameter.	6.1	More Details
CVE-2020-21495	A cross-site scripting (XSS) vulnerability in the component /admin/?setting-base.htm of Xiuno BBS 4.0.4 allows attackers to execute arbitrary web scripts or HTML via the sitename parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24676	The Better Find and Replace WordPress plugin before 1.2.9 does not escape the 's' GET parameter before outputting back in the All Masking Rules page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2020-21505	waimai Super Cms 20150505 contains a cross-site scripting (XSS) vulnerability in the component /admin.php/Link/addsave.	6.1	More Details
CVE-2021-24679	The Bitcoin / AltCoin Payment Gateway for WooCommerce WordPress plugin before 1.6.1 does not escape the 's' GET parameter before outputting back in the All Masking Rules page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2020-21496	A cross-site scripting (XSS) vulnerability in the component /admin/?setting-base.htm of Xiuno BBS 4.0.4 allows attackers to execute arbitrary web scripts or HTML via the sitebrief parameter.	6.1	More Details
CVE-2021-41878	A reflected cross-site scripting (XSS) vulnerability exists in the i-Panel Administration System Version 2.0 that enables a remote attacker to execute arbitrary JavaScript code in the browser-based web console and it is possible to insert a vulnerable malicious button.	6.1	More Details
CVE-2021-20554	IBM Sterling Order Management 9.4, 9.5, and 10.0 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: 199179.	6.1	More Details
CVE-2021-41555	In ARCHIBUS Web Central 21.3.3.815 (a version from 2014), XSS occurs in /archibus/dwr/call/plaincall/workflow.runWorkflowRule.dwr because the data received as input from clients is re-included within the HTTP response returned by the application without adequate validation. In this way, if HTML code or client-side executable code (e.g., Javascript) is entered as input, the expected execution flow could be altered. This is fixed in all recent versions, such as version 26. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Version 21.3 was officially de-supported by the end of 2020	6.1	More Details
CVE-2020-21504	waimai Super Cms 20150505 contains a cross-site scripting (XSS) vulnerability in the component /admin.php?&m=Public&a=login.	6.1	More Details
CVE-2020-28119	Cross site scripting vulnerability in 53KF < 2.0.0.2 that allows for arbitrary code to be executed via crafted HTML statement inserted into chat window.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39846	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a stack overflow vulnerability due to insecure handling of a crafted PDF file, potentially resulting in memory corruption in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted PDF file in Acrobat Reader.	6.1	More Details
CVE-2021-40975	Cross-site scripting (XSS) vulnerability in application/modules/admin/views/ecommerce/products.php in Ecommerce-CodeIgniter-Bootstrap (Codeigniter 3.1.11, Bootstrap 3.3.7) allows remote attackers to inject arbitrary web script or HTML via the search_title parameter.	6.1	More Details
CVE-2021-25963	In Shuup, versions 1.6.0 through 2.10.8 are vulnerable to reflected Cross-Site Scripting (XSS) that allows execution of arbitrary javascript code on a victim browser. This vulnerability exists due to the error page contents not escaped.	6.1	More Details
CVE-2020-21506	waimai Super Cms 20150505 contains a cross-site scripting (XSS) vulnerability in the component /admin.php?m=Config&a=add.	6.1	More Details
CVE-2021-39845	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a stack overflow vulnerability due to insecure handling of a crafted PDF file, potentially resulting in memory corruption in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted PDF file in Acrobat Reader.	6.1	More Details
CVE-2021-40972	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the mail parameter.	6.1	More Details
CVE-2021-41462	Cross-site scripting (XSS) vulnerability in concrete/elements/collection_add.php in concrete5-legacy 5.6.4.0 and below allows remote attackers to inject arbitrary web script or HTML via the ctID parameter.	6.1	More Details
CVE-2021-41463	Cross-site scripting (XSS) vulnerability in toos/permissions/dialogs/access/entity/types/group_combination.php in concrete5-legacy 5.6.4.0 and below allows remote attackers to inject arbitrary web script or HTML via the cID parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41464	Cross-site scripting (XSS) vulnerability in concrete/elements/collection_add.php in concrete5-legacy 5.6.4.0 and below allows remote attackers to inject arbitrary web script or HTML via the rel parameter.	6.1	More Details
CVE-2021-41465	Cross-site scripting (XSS) vulnerability in concrete/elements/collection_theme.php in concrete5-legacy 5.6.4.0 and below allows remote attackers to inject arbitrary web script or HTML via the rel parameter.	6.1	More Details
CVE-2021-41467	Cross-site scripting (XSS) vulnerability in application/controllers/dropbox.php in JustWriting 1.0.0 and below allow remote attackers to inject arbitrary web script or HTML via the challenge parameter.	6.1	More Details
CVE-2021-40971	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the newpassword1 parameter.	6.1	More Details
CVE-2021-40970	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the username parameter.	6.1	More Details
CVE-2021-40969	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the firstname parameter.	6.1	More Details
CVE-2021-40968	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the newpassword2 parameter.	6.1	More Details
CVE-2021-40928	Cross-site scripting (XSS) vulnerability in index.php in FlexTV beta development version allows remote attackers to inject arbitrary web script or HTML via the PHP_SELF parameter.	6.1	More Details
CVE-2021-40927	Cross-site scripting (XSS) vulnerability in callback.php in Spotify-for-Alfred 0.13.9 and below allows remote attackers to inject arbitrary web script or HTML via the error parameter.	6.1	More Details
CVE-2021-40926	Cross-site scripting (XSS) vulnerability in demos/demo.mysqli.php in getID3 1.X and v2.0.0-beta allows remote attackers to inject arbitrary web script or HTML via the showtagfiles parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40925	Cross-site scripting (XSS) vulnerability in dompdf/dompdf/www/demo.php infaveo-helpdesk v1.11.0 and below allow remote attackers to inject arbitrary web script or HTML via the $_SERVER["PHP_SELF"] parameter.	6.1	More Details
CVE-2020-21228	JIZHICMS 1.5.1 contains a cross-site scripting (XSS) vulnerability in the component /user/release.html, which allows attackers to arbitrarily add an administrator cookie.	6.1	More Details
CVE-2021-40924	Cross-site scripting (XSS) vulnerability in install/index.php in bugs 1.8 and below version allows remote attackers to inject arbitrary web script or HTML via the first_name parameter.	6.1	More Details
CVE-2021-40923	Cross-site scripting (XSS) vulnerability in install/index.php in bugs 1.8 and below version allows remote attackers to inject arbitrary web script or HTML via the email parameter.	6.1	More Details
CVE-2021-40922	Cross-site scripting (XSS) vulnerability in install/index.php in bugs 1.8 and below version allows remote attackers to inject arbitrary web script or HTML via the last_name parameter.	6.1	More Details
CVE-2021-40921	Cross-site scripting (XSS) vulnerability in _contactform.inc.php in Detector 0.8.5 and below version allows remote attackers to inject arbitrary web script or HTML via the cid parameter.	6.1	More Details
CVE-2021-29109	A reflected XSS vulnerability in Esri Portal for ArcGIS version 10.9 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser.	6.1	More Details
CVE-2021-35503	Afian FileRun 2021.03.26 allows stored XSS via an HTTP X-Forwarded-For header that is mishandled when rendering Activity Logs.	6.1	More Details
CVE-2021-41826	PlaceOS Authentication Service before 1.29.10.0 allows app/controllers/auth/sessions_controller.rb open redirect.	6.1	More Details
CVE-2021-41461	Cross-site scripting (XSS) vulnerability in concrete/elements/collection_add.php in concrete5-legacy 5.6.4.0 and below allows remote attackers to inject arbitrary web script or HTML via the mode parameter.	6.1	More Details
CVE-2021-39891	In all versions of GitLab CE/EE since version 8.0, access tokens created as part of admin's impersonation of a user are not cleared at the end of impersonation which may lead to unnecessary sensitive info disclosure.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22947	When curl >= 7.20.0 and <= 7.78.0 connects to an IMAP or POP3 server to retrieve data using STARTTLS to upgrade to TLS security, the server can respond and send back multiple responses at once that curl caches. curl would then upgrade to TLS but not flush the in-queue of cached responses but instead continue using and trustingthe responses it got *before* the TLS handshake as if they were authenticated.Using this flaw, it allows a Man-In-The-Middle attacker to first inject the fake responses, then pass-through the TLS traffic from the legitimate server and trick curl into sending data back to the user thinking the attacker's injected data comes from the TLS-protected server.	5.9	More Details
CVE-2021-39878	A stored Reflected Cross-Site Scripting vulnerability in the Jira integration in GitLab version 13.0 up to 14.3.1 allowed an attacker to execute arbitrary javascript code.	5.8	More Details
CVE-2021-35203	NETSCOUT Systems nGeniusONE 6.3.0 build 1196 allows Arbitrary File Read operations via the FDSQueryService endpoint.	5.7	More Details
CVE-2021-41101	wire-server is an open-source back end for Wire, a secure collaboration platform. Before version 2.106.0, the CORS ` Access-Control-Allow-Origin ` header set by `nginz` is set for all subdomains of `.wire.com` (including `wire.com`). This means that if somebody were to find an XSS vector in any of the subdomains, they could use it to talk to the Wire API using the user's Cookie. A patch does not exist, but a workaround does. To make sure that a compromise of one subdomain does not yield access to the cookie of another, one may limit the `Access-Control-Allow-Origin` header to apps that actually require the cookie (account-pages, team-settings and the webapp).	5.7	More Details
CVE-2021-33923	Insecure permissions in Confluent Ansible (cp-ansible) 5.5.0, 5.5.1, 5.5.2 and 6.0.0 allows local attackers to access some sensitive information (private keys, state database).	5.5	More Details
CVE-2021-38106	UAX200.dll in Corel Presentations 2020 20.0.0.200 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PPT file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38102	IPPP82.FLT in Corel Presentations 2020 20.0.0.200 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PPT file. This is different from CVE-2021-38105.	5.5	More Details
CVE-2021-38109	Corel DrawStandard 2020 22.0.0.474 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious CDR file.	5.5	More Details
CVE-2021-38108	Word97Import200.dll in Corel WordPerfect 2020 20.0.0.200 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious DOC file.	5.5	More Details
CVE-2021-39860	Acrobat Pro DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive user memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-38107	CdrCore.dll in Corel DrawStandard 2020 22.0.0.474 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious CDR file.	5.5	More Details
CVE-2021-39849	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39850	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-39851	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-39852	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-39861	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of 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.	5.5	More Details
CVE-2021-39853	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-38105	IPPP82.FLT in Corel Presentations 2020 20.0.0.200 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PPT file. This is different from CVE-2021-38102.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40716	XMP Toolkit SDK versions 2021.07 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive 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.	5.5	More Details
CVE-2021-38104	IPPP72.FLT in Corel Presentations 2020 20.0.0.200 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PPT file.	5.5	More Details
CVE-2021-35198	NETSCOUT nGeniusONE 6.3.0 build 1004 and earlier allows Stored Cross-Site Scripting (XSS) in the Packet Analysis module.	5.4	More Details
CVE-2021-29110	Stored cross-site scripting (XSS) issue in Esri Portal for ArcGIS may allow a remote unauthenticated attacker to pass and store malicious strings in the home application.	5.4	More Details
CVE-2021-22262	Missing access control in all GitLab versions starting from 13.12 before 14.0.9, all versions starting from 14.1 before 14.1.4, and all versions starting from 14.2 before 14.2.2 with Jira Cloud integration enabled allows Jira users without administrative privileges to add and remove Jira Connect Namespaces via the GitLab.com for Jira Cloud application configuration page	5.4	More Details
CVE-2021-35199	NETSCOUT nGeniusONE 6.3.0 build 1196 and earlier allows Stored Cross-Site Scripting (XSS) in UploadFile.	5.4	More Details
CVE-2021-38675	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Image2PDF. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Image2PDF: Image2PDF 2.1.5 (2021/08/17) and later	5.4	More Details
CVE-2020-20799	JeeCMS 1.0.1 contains a stored cross-site scripting (XSS) vulnerability which allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the commentText parameter.	5.4	More Details
CVE-2021-35205	NETSCOUT Systems nGeniusONE version 6.3.0 build 1196 allows URL redirection in redirector.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41092	Docker CLI is the command line interface for the docker container runtime. A bug was found in the Docker CLI where running `docker login my-private-registry.example.com` with a misconfigured configuration file (typically `~/.docker/config.json`) listing a `credsStore` or `credHelpers` that could not be executed would result in any provided credentials being sent to `registry-1.docker.io` rather than the intended private registry. This bug has been fixed in Docker CLI 20.10.9. Users should update to this version as soon as possible. For users unable to update ensure that any configured credsStore or credHelpers entries in the configuration file reference an installed credential helper that is executable and on the PATH.	5.4	More Details
CVE-2021-35204	NETSCOUT Systems nGeniusONE 6.3.0 build 1196 allows Reflected Cross-Site Scripting (XSS) in the support endpoint.	5.4	More Details
CVE-2021-24017	An improper authentication in Fortinet FortiManager version 6.4.3 and below, 6.2.6 and below allows attacker to assign arbitrary Policy and Object modules via crafted requests to the request handler.	5.4	More Details
CVE-2021-24654	The User Registration WordPress plugin before 2.0.2 does not properly sanitise the user_registration_profile_pic_url value when submitted directly via the user_registration_update_profile_details AJAX action. This could allow any authenticated user, such as subscriber, to perform Stored Cross-Site attacks when their profile is viewed	5.4	More Details
CVE-2021-38822	A Stored Cross Site Scripting vulnerability via Malicious File Upload exists in multiple pages of IceHrm 30.0.0.OS that allows for arbitrary execution of JavaScript commands.	5.4	More Details
CVE-2020-20129	LaraCMS v1.0.1 contains a stored cross-site scripting (XSS) vulnerability which allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the content editor.	5.4	More Details
CVE-2021-33849	A Cross-Site Scripting (XSS) attack can cause arbitrary code (JavaScript) to run in a user’s browser while the browser is connected to a trusted website. The attack targets your application's users and not the application itself while using your application as the attack's vehicle. The XSS payload executes whenever the user changes the form values or deletes a created form in Zoho CRM Lead Magnet Version 1.7.2.4.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29834	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3,20.0.0.1, 20.0.0.2, and 21.0.2 and IBM Business Process Manager 8.5 and 8.6 are vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204832.	5.4	More Details
CVE-2021-39866	A business logic error in the project deletion process in GitLab 13.6 and later allows persistent access via project access tokens.	5.4	More Details
CVE-2021-36850	Cross-Site Request Forgery (CSRF) vulnerability in WordPress Media File Renamer – Auto & Manual Rename plugin (versions <= 5.1.9). Affected parameters "post_title", "filename", "lock". This allows changing the uploaded media title, media file name, and media locking state.	5.4	More Details
CVE-2021-25964	In “Calibre-web” application, v0.6.0 to v0.6.12, are vulnerable to Stored XSS in “Metadata”. An attacker that has access to edit the metadata information, can inject JavaScript payload in the description field. When a victim tries to open the file, XSS will be triggered.	5.4	More Details
CVE-2021-39486	A Stored XSS via Malicious File Upload exists in Gila CMS version 2.2.0. An attacker can use this to steal cookies, passwords or to run arbitrary code on a victim's browser.	5.4	More Details
CVE-2021-39894	In all versions of GitLab CE/EE since version 8.0, a DNS rebinding vulnerability exists in Fogbugz importer which may be used by attackers to exploit Server Side Request Forgery attacks.	5.4	More Details
CVE-2020-21434	Maccms 10 contains a cross-site scripting (XSS) vulnerability in the Editing function under the Member module. This vulnerability is exploited via a crafted payload in the nickname text field.	5.4	More Details
CVE-2021-37330	Laravel Booking System Booking Core 2.0 is vulnerable to Cross Site Scripting (XSS). The Avatar upload in the My Profile section could be exploited to upload a malicious SVG file which contains Javascript. Now if another user/admin views the profile and clicks to view his avatar, an XSS will trigger.	5.4	More Details
CVE-2020-20131	LaraCMS v1.0.1 contains a stored cross-site scripting (XSS) vulnerability which allows atackers to execute arbitrary web scripts or HTML via a crafted payload in the page management module.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24678	The CM Tooltip Glossary WordPress plugin before 3.9.21 does not escape some glossary_tooltip shortcode attributes, which could allow users a role as low as Contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2020-20781	A stored cross-site scripting (XSS) vulnerability in /ucms/index.php?do=list_edit of UCMS 1.4.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the title, key words, description or content text fields.	5.4	More Details
CVE-2021-39342	The Credova_Financial WordPress plugin discloses a site's associated Credova API account username and password in plaintext via an AJAX action whenever a site user goes to checkout on a page that has the Credova Financing option enabled. This affects versions up to, and including, 1.4.8.	5.3	More Details
CVE-2021-39882	In all versions of GitLab CE/EE, provided a user ID, anonymous users can use a few endpoints to retrieve information about any GitLab user.	5.3	More Details
CVE-2021-39893	A potential DOS vulnerability was discovered in GitLab starting with version 9.1 that allowed parsing files without authorisation.	5.3	More Details
CVE-2020-21493	An issue in the component route\user.php of Xiuno BBS v4.0.4 allows attackers to enumerate usernames.	5.3	More Details
CVE-2021-22257	An issue has been discovered in GitLab affecting all versions starting from 14.0 before 14.0.9, all versions starting from 14.1 before 14.1.4, all versions starting from 14.2 before 14.2.2. The route for /user.keys is not restricted on instances with public visibility disabled. This allows user enumeration on such instances.	5.3	More Details
CVE-2021-41123	Survey Solutions is a survey management and data collection system. In affected versions the Headquarters application publishes /metrics endpoint available to any user. None of the survey answers are ever exposed, only the aggregate counters, including count of interviews, or count of assignments. Starting from version 21.09.1 the endpoint is turned off by default.	5.3	More Details
CVE-2021-39875	In all versions of GitLab CE/EE since version 13.6, it is possible to see pending invitations of any public group or public project by visiting an API endpoint.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32672	Redis is an open source, in-memory database that persists on disk. When using the Redis Lua Debugger, users can send malformed requests that cause the debugger's protocol parser to read data beyond the actual buffer. This issue affects all versions of Redis with Lua debugging support (3.2 or newer). The problem is fixed in versions 6.2.6, 6.0.16 and 5.0.14.	5.3	More Details
CVE-2021-41118	The DynamicPageList3 extension is a reporting tool for MediaWiki, listing category members and intersections with various formats and details. In affected versions unsanitised input of regular expression date within the parameters of the DPL parser function, allowed for the possibility of ReDoS (Regex Denial of Service). This has been resolved in version 3.3.6. If you are unable to update you may also set `$wgDplSettings['functionalRichness'] = 0;` or disable DynamicPageList3 to mitigate.	5.3	More Details
CVE-2021-21706	In PHP versions 7.3.x below 7.3.31, 7.4.x below 7.4.24 and 8.0.x below 8.0.11, in Microsoft Windows environment, ZipArchive::extractTo may be tricked into writing a file outside target directory when extracting a ZIP file, thus potentially causing files to be created or overwritten, subject to OS permissions.	5.3	More Details
CVE-2021-22557	SLO generator allows for loading of YAML files that if crafted in a specific format can allow for code execution within the context of the SLO Generator. We recommend upgrading SLO Generator past https://github.com/google/slo-generator/pull/173	5.3	More Details
CVE-2021-41867	An information disclosure vulnerability in OnionShare 2.3 before 2.4 allows remote unauthenticated attackers to retrieve the full list of participants of a non-public OnionShare node via the --chat feature.	5.3	More Details
CVE-2021-37331	Laravel Booking System Booking Core 2.0 is vulnerable to Incorrect Access Control. On the Verifications page, after uploading an ID Card or Trade License and viewing it, ID Cards and Trade Licenses of other vendors/users can be viewed by changing the URL.	5.3	More Details
CVE-2021-41596	SuiteCRM before 7.10.33 and 7.11.22 allows information disclosure via Directory Traversal. An attacker can partially include arbitrary files via the importFile parameter of the RefreshMapping import functionality.	5.3	More Details
CVE-2021-41595	SuiteCRM before 7.10.33 and 7.11.22 allows information disclosure via Directory Traversal. An attacker can partially include arbitrary files via the file_name parameter of the Step3 import functionality.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21704	In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using Firebird PDO driver extension, a malicious database server could cause crashes in various database functions, such as getAttribute(), execute(), fetch() and others by returning invalid response data that is not parsed correctly by the driver. This can result in crashes, denial of service or potentially memory corruption.	5.0	More Details
CVE-2021-41114	TYPO3 is an open source PHP based web content management system released under the GNU GPL. It has been discovered that TYPO3 CMS is susceptible to host spoofing due to improper validation of the HTTP Host header. TYPO3 uses the HTTP Host header, for example, to generate absolute URLs during the frontend rendering process. Since the host header itself is provided by the client, it can be forged to any value, even in a name-based virtual hosts environment. This vulnerability is the same as described in TYPO3-CORE-SA-2014-001 (CVE-2014-3941). A regression, introduced during TYPO3 v11 development, led to this situation. The already existing setting $GLOBALS['TYPO3_CONF_VARS']['SYS']['trustedHostsPattern'] (used as an effective mitigation strategy in previous TYPO3 versions) was not evaluated anymore, and reintroduced the vulnerability.	4.8	More Details
CVE-2021-24673	The Appointment Hour Booking WordPress plugin before 1.3.16 does not escape some of the Calendar Form settings, allowing high privilege users to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-35200	NETSCOUT nGeniusONE 6.3.0 build 1196 allows high-privileged users to achieve Stored Cross-Site Scripting (XSS) in FDSQueryService.	4.8	More Details
CVE-2021-24687	The Modern Events Calendar Lite WordPress plugin before 5.22.2 does not escape some of its settings before outputting them in attributes, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-39884	In all versions of GitLab EE since version 8.13, an endpoint discloses names of private groups that have access to a project to low privileged users that are part of that project.	4.3	More Details
CVE-2021-3436	BT: Possible to overwrite an existing bond during keys distribution phase when the identity address of the bond is known. Zephyr versions >= 1.14.2, >= 2.4.0, >= 2.5.0 contain Use of Multiple Resources with Duplicate Identifier (CWE-694). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-j76f-35mc-4h63	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22258	The project import/export feature in GitLab 8.9 and greater could be used to obtain otherwise private email addresses	4.3	More Details
CVE-2021-39888	In all versions of GitLab EE starting from 13.10 before 14.1.7, all versions starting from 14.2 before 14.2.5, and all versions starting from 14.3 before 14.3.1 a specific API endpoint may reveal details about a private group and other sensitive info inside issue and merge request templates.	4.3	More Details
CVE-2021-39889	In all versions of GitLab EE since version 14.1, due to an insecure direct object reference vulnerability, an endpoint may reveal the protected branch name to a malicious user who makes a crafted API call with the ID of the protected branch.	4.3	More Details
CVE-2021-39870	In all versions of GitLab CE/EE since version 11.11, an instance that has the setting to disable Repo by URL import enabled is bypassed by an attacker making a crafted API call.	4.3	More Details
CVE-2021-39871	In all versions of GitLab CE/EE since version 13.0, an instance that has the setting to disable Bitbucket Server import enabled is bypassed by an attacker making a crafted API call.	4.3	More Details
CVE-2021-41122	Vyper is a Pythonic Smart Contract Language for the EVM. In affected versions external functions did not properly validate the bounds of decimal arguments. The can lead to logic errors. This issue has been resolved in version 0.3.0.	4.3	More Details
CVE-2021-39874	In all versions of GitLab CE/EE since version 11.0, the requirement to enforce 2FA is not honored when using git commands.	4.3	More Details
CVE-2021-39868	In all versions of GitLab CE/EE since version 8.12, an authenticated low-privileged malicious user may create a project with unlimited repository size by modifying values in a project export.	4.3	More Details
CVE-2021-39883	Improper authorization checks in all versions of GitLab EE starting from 13.11 before 14.1.7, all versions starting from 14.2 before 14.2.5, and all versions starting from 14.3 before 14.3.1 allows subgroup members to see epics from all parent subgroups.	4.3	More Details
CVE-2021-39873	In all versions of GitLab CE/EE, there exists a content spoofing vulnerability which may be leveraged by attackers to trick users into visiting a malicious website by spoofing the content in an error response.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35202	NETSCOUT Systems nGeniusONE 6.3.0 build 1196 allows Authorization Bypass (to access an endpoint) in FDSQueryService.	4.3	More Details
CVE-2021-22259	A potential DOS vulnerability was discovered in GitLab EE starting with version 12.6 due to lack of pagination in dependencies API.	4.3	More Details
CVE-2021-21705	In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using URL validation functionality via filter_var() function with FILTER_VALIDATE_URL parameter, an URL with invalid password field can be accepted as valid. This can lead to the code incorrectly parsing the URL and potentially leading to other security implications - like contacting a wrong server or making a wrong access decision.	4.3	More Details
CVE-2021-39347	The Stripe for WooCommerce WordPress plugin is missing a capability check on the save() function found in the ~/includes/admin/class-wc-stripe-admin-user-edit.php file that makes it possible for attackers to configure their account to use other site users unique STRIPE identifier and make purchases with their payment accounts. This affects versions 3.0.0 - 3.3.9.	4.3	More Details
CVE-2021-41094	Wire is an open source secure messenger. Users of Wire by Bund may bypass the mandatory encryption at rest feature by simply disabling their device passcode. Upon launching, the app will attempt to enable encryption at rest by generating encryption keys via the Secure Enclave, however it will fail silently if no device passcode is set. The user has no indication that encryption at rest is not active since the feature is hidden to them. This issue has been resolved in version 3.70	4.2	More Details
CVE-2021-39896	In all versions of GitLab CE/EE since version 8.0, when an admin uses the impersonate feature twice and stops impersonating, the admin may be logged in as the second user they impersonated, which may lead to repudiation issues.	3.8	More Details
CVE-2021-24016	An improper neutralization of formula elements in a csv file in Fortinet FortiManager version 6.4.3 and below, 6.2.7 and below allows attacker to execute arbitrary commands via crafted IPv4 field in policy name, when exported as excel file and opened unsafely on the victim host.	3.7	More Details
CVE-2021-39881	In all versions of GitLab CE/EE since version 7.7, the application may let a malicious user create an OAuth client application with arbitrary scope names which may allow the malicious user to trick unsuspecting users to authorize the malicious client application using the spoofed scope name and description.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41861	The Telegram application 7.5.0 through 7.8.0 for Android does not properly implement image self-destruction, a different vulnerability than CVE-2019-16248. After approximately two to four uses of the self-destruct feature, there is a misleading UI indication that an image was deleted (on both the sender and recipient sides). The images are still present in the /Storage/Emulated/0/Telegram/Telegram Image/ directory.	3.3	More Details
CVE-2021-39844	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of 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-2021-21089	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 Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally escalate privileges 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-2021-39899	In all versions of GitLab CE/EE, an attacker with physical access to a user’s machine may brute force the user’s password via the change password function. There is a rate limit in place, but the attack may still be conducted by stealing the session id from the physical compromise of the account and splitting the attack over several IP addresses and passing in the compromised session value from these various locations.	2.9	More Details
CVE-2021-41089	Moby is an open-source project created by Docker to enable software containerization. A bug was found in Moby (Docker Engine) where attempting to copy files using `docker cp` into a specially-crafted container can result in Unix file permission changes for existing files in the host’s filesystem, widening access to others. This bug does not directly allow files to be read, modified, or executed without an additional cooperating process. This bug has been fixed in Moby (Docker Engine) 20.10.9. Users should update to this version as soon as possible. Running containers do not need to be restarted.	2.8	More Details
CVE-2021-39886	Permissions rules were not applied while issues were moved between projects of the same group in GitLab versions starting with 10.6 and up to 14.1.7 allowing users to read confidential Epic references.	2.6	More Details
CVE-2021-39879	Missing authentication in all versions of GitLab CE/EE since version 7.11.0 allows an attacker with access to a victim's session to disable two-factor authentication	2.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39900	Information disclosure from SendEntry in GitLab starting with 10.8 allowed exposure of full URL of artifacts stored in object-storage with a temporary availability via Rails logs.	2.0	More Details
CVE-2021-39835	Adobe Framemaker versions 2019 Update 8 (and earlier) and 2020 Release Update 2 (and earlier) are affected by a use-after-free vulnerability in the processing of a malformed PDF file that could result in disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious PDF file.	N/A	More Details
CVE-2021-40697	Adobe Framemaker versions 2019 Update 8 (and earlier) and 2020 Release Update 2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive 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.	N/A	More Details
CVE-2021-28547	Adobe Creative Cloud Desktop Application for macOS version 5.3 (and earlier) is affected by a privilege escalation vulnerability that could allow a normal user to delete the OOBE directory and get permissions of any directory under the administrator authority.	N/A	More Details
CVE-2021-40710	Adobe Premiere Pro version 15.4 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious .svg file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required in that the victim must open a specially crafted file to exploit this vulnerability.	N/A	More Details
CVE-2021-39821	Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier) are affected by an out-of-bounds read 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 TIF file.	N/A	More Details
CVE-2021-39829	Adobe Framemaker versions 2019 Update 8 (and earlier) and 2020 Release Update 2 (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 PDF file.	N/A	More Details
CVE-2021-39830	Adobe Framemaker versions 2019 Update 8 (and earlier) and 2020 Release Update 2 (and earlier) are affected by a memory corruption vulnerability due to insecure handling of a malicious PDF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39832	Adobe Framemaker versions 2019 Update 8 (and earlier) and 2020 Release Update 2 (and earlier) are affected by a memory corruption vulnerability due to insecure handling of a malicious PDF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details
CVE-2021-39833	Adobe Framemaker versions 2019 Update 8 (and earlier) and 2020 Release Update 2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive 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 TIF file.	N/A	More Details
CVE-2021-39834	Adobe Framemaker versions 2019 Update 8 (and earlier) and 2020 Release Update 2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive 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 TIF file.	N/A	More Details
CVE-2021-39837	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability in the processing of the AcroForm deleteItemAt action that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-39858	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of 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.	N/A	More Details
CVE-2021-39838	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability in the processing of the AcroForm buttonGetCaption action that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39854	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2021-39839	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability in the processing of the AcroForm getItem action that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-39840	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability when processing AcroForms that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	N/A	More Details
CVE-2021-41720	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-39841	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a Type Confusion vulnerability. An attacker could leverage this vulnerability to execute arbitrary code 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-2021-39842	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (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.	N/A	More Details
CVE-2021-39857	Adobe Acrobat Reader DC add-on for Internet Explorer versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to check for existence of local files. Exploitation of this issue requires user interaction in that a victim must visit an attacker controlled web page.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39865	Adobe Framemaker versions 2019 Update 8 (and earlier) and 2020 Release Update 2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive 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.	N/A	More Details
CVE-2021-39862	Adobe Framemaker versions 2019 Update 8 (and earlier) and 2020 Release Update 2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive 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.	N/A	More Details