SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 13 July 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-31125	Roxy-wi is an open source web interface for managing Haproxy, Nginx, Apache and Keepalived servers. A vulnerability in Roxy-wi allows a remote, unauthenticated attacker to bypass authentication and access admin functionality by sending a specially crafted HTTP request. This affects Roxywi versions before 6.1.1.0. Users are advised to upgrade. There are no known workarounds for this issue.	10.0	More Details
CVE-2022-31126	Roxy-wi is an open source web interface for managing Haproxy, Nginx, Apache and Keepalived servers. A vulnerability in Roxy-wi allows a remote, unauthenticated attacker to code execution by sending a specially crafted HTTP request to /app/options.py file. This affects Roxy-wi versions before 6.1.1.0. Users are advised to upgrade. There are no known workarounds for this issue.	10.0	More Details
CVE-2021-41037	In Eclipse p2, installable units are able to alter the Eclipse Platform installation and the local machine via touchpoints during installation. Those touchpoints can, for example, alter the command-line used to start the application, injecting things like agent or other settings that usually require particular attention in term of security. Although p2 has built-in strategies to ensure artifacts are signed and then to help establish trust, there is no such strategy for the metadata part that does configure such touchpoints. As a result, it's possible to install a unit that will run malicious code during installation without user receiving any warning about this installation step being risky when coming from untrusted source.	10.0	More Details
CVE-2022-34819	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions < V3.3.46), SIMATIC CP 1243-1 (All versions < V3.3.46), SIMATIC CP 1243-7 LTE EU (All versions < V3.3.46), SIMATIC CP 1243-7 LTE US (All versions < V3.3.46), SIMATIC CP 1243-8 IRC (All versions < V3.3.46), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0 < V2.2.28), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0 < V2.2.28), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0 < V2.2.28), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0 < V2.2.28), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0 < V2.2.28), SIPLUS NET CP 1242-7 V2 (All versions < V3.3.46), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions < V3.3.46), SIPLUS S7-1200 CP 1243-1 RAIL (All versions < V3.3.46). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device.	10.0	More Details
CVE-2022-31137	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Versions prior to 6.1.1.0 are subject to a remote code execution vulnerability. System commands can be run remotely via the subprocess_execute function without processing the inputs received from the user in the /app/options.py file. Attackers need not be authenticated to exploit this vulnerability. Users are advised to upgrade. There are no known workarounds for this vulnerability.	10.0	More Details
CVE-2021-35283	SQL Injection vulnerability in product_admin.php in atoms183 CMS 1.0, allows attackers to execute arbitrary commands via the Name, Fname, and ID parameters to search.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1245	A privilege escalation flaw was found in the token exchange feature of keycloak. Missing authorization allows a client application holding a valid access token to exchange tokens for any target client by passing the client_id of the target. This could allow a client to gain unauthorized access to additional services.	9.8	More Details
CVE-2022-28623	Security vulnerabilities in HPE IceWall SSO 10.0 certd could be exploited remotely to allow SQL injection or unauthorized data injection. HPE has provided the following updated modules to resolve these vulnerabilities. HPE IceWall SSO version 10.0 certd library Patch 9 for RHEL and HPE IceWall SSO version 10.0 certd library Patch 9 for HP-UX.	9.8	More Details
CVE-2022-34914	Webswing before 22.1.3 allows X-Forwarded-For header injection. The client IP address is associated with a variable in the configuration page. The {clientIp} variable can be used as an application startup argument. The X-Forwarded-For header can be manipulated by a client to store an arbitrary value that is used to replace the clientIp variable (without sanitization). A client can thus inject multiple arguments into the session startup. Systems that do not use the clientIP variable in the configuration are not vulnerable. The vulnerability is fixed in these versions: 20.1.16, 20.2.19, 21.1.8, 21.2.12, and 22.1.3.	9.8	More Details
CVE-2022-35411	rpc.py through 0.6.0 allows Remote Code Execution because an unpickle occurs when the "serializer: pickle" HTTP header is sent. In other words, although JSON (not Pickle) is the default data format, an unauthenticated client can cause the data to be processed with unpickle.	9.8	More Details
CVE-2022-32383	Tenda AC23 v16.03.07.44 was discovered to contain a stack overflow via the AdvSetMacMtuWan function.	9.8	More Details
CVE-2022-31570	The adriankoczuruek/ceneo-web-scrapper repository through 2021-03-15 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.8	More Details
CVE-2022-32533	Apache Jetspeed-2 does not sufficiently filter untrusted user input by default leading to a number of issues including XSS, CSRF, XXE, and SSRF. Setting the configuration option "xss.filter.post = true" may mitigate these issues. NOTE: Apache Jetspeed is a dormant project of Apache Portals and no updates will be provided for this issue	9.8	More Details
CVE-2022-34592	Wavlink WL-WN575A3 RPT75A3.V4300.201217 was discovered to contain a command injection vulnerability via the function obtw. This vulnerability allows attackers to execute arbitrary commands via a crafted POST request.	9.8	More Details
CVE-2022-32294	Zimbra Collaboration Open Source 8.8.15 does not encrypt the initial-login randomly created password (from the "zmprove ca" command). It is visible in cleartext on port UDP 514 (aka the syslog port). NOTE: a third party reports that this cannot be reproduced.	9.8	More Details
CVE-2022-2302	Multiple Lenze products of the cabinet series skip the password verification upon second login. After a user has been logged on to the device once, a remote attacker can get full access without knowledge of the password.	9.8	More Details
CVE-2022-1057	The Pricing Deals for WooCommerce WordPress plugin through 2.0.2.02 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to an unauthenticated SQL injection	9.8	More Details
CVE-2022-1952	The Free Booking Plugin for Hotels, Restaurant and Car Rental WordPress plugin before 1.1.16 suffers from insufficient input validation which leads to arbitrary file upload and subsequently to remote code execution. An AJAX action accessible to unauthenticated users is affected by this issue. An allowlist of valid file extensions is defined but is not used during the validation steps.	9.8	More Details
CVE-2020-4150	IBM SiteProtector Appliance 3.1.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174142.	9.8	More Details
CVE-2022-1737	Pyramid Solutions' affected products, the Developer and DLL kits for EtherNet/IP Adapter and EtherNet/IP Scanner, are vulnerable to an out-of-bounds write, which may allow an unauthorized attacker to send a specially crafted packet that may result in a denial-of-service condition.	9.8	More Details
CVE-2022-29600	The oelib (aka One is Enough Library) extension through 4.1.5 for TYPO3 allows SQL Injection.	9.8	More Details
CVE-2022-29601	The seminars (aka Seminar Manager) extension through 4.1.3 for TYPO3 allows SQL Injection.	9.8	More Details
CVE-2021-29281	File upload vulnerability in GFI Mail Archiver versions up to and including 15.1 via insecure implementation of Telerik Web UI plugin which is affected by CVE-2014-2217, and CVE-2017-11317.	9.8	More Details
CVE-2022-35628	A SQL injection issue was discovered in the lux extension before 17.6.1, and 18.x through 24.x before 24.0.2, for TYPO3.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32449	TOTOLINK EX300_V2 V4.0.3c.7484 was discovered to contain a command injection vulnerability via the langType parameter in the setLanguageCfg function. This vulnerability is exploitable via a crafted MQTT data packet.	9.8	More Details
CVE-2022-20083	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883.	9.8	More Details
CVE-2022-33047	OTFCC v0.10.4 was discovered to contain a heap buffer overflow after free via otfccbuild.c.	9.8	More Details
CVE-2022-34598	The udpserver in H3C Magic R100 V200R004 and V100R005 has the 9034 port opened, allowing attackers to execute arbitrary commands.	9.8	More Details
CVE-2022-34597	Tenda AX1806 v1.0.0.1 was discovered to contain a command injection vulnerability via the function WanParameterSetting.	9.8	More Details
CVE-2022-34596	Tenda AX1803 v1.0.0.1_2890 was discovered to contain a command injection vulnerability via the function WanParameterSetting.	9.8	More Details
CVE-2022-34595	Tenda AX1803 v1.0.0.1_2890 was discovered to contain a command injection vulnerability via the function setipv6status.	9.8	More Details
CVE-2022-21744	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626.	9.8	More Details
CVE-2022-32056	Online Accreditation Management v1.0 was discovered to contain a SQL injection vulnerability via the USERNAME parameter at process.php.	9.8	More Details
CVE-2022-32386	Tenda AC23 v16.03.07.44 was discovered to contain a buffer overflow via fromAdvSetMacMtuWan.	9.8	More Details
CVE-2022-25046	A path traversal vulnerability in loader.php of CWP v0.9.8.1122 allows attackers to execute arbitrary code via a crafted POST request.	9.8	More Details
CVE-2022-32207	When curl < 7.84.0 saves cookies, alt-svc and hsts data to local files, it makes the operation atomic by finalizing the operation with a rename from a temporary name to the final target file name.In that rename operation, it might accidentally *widen* the permissions for the target file, leaving the updated file accessible to more users than intended.	9.8	More Details
CVE-2022-32385	Tenda AC23 v16.03.07.44 is vulnerable to Stack Overflow that will allow for the execution of arbitrary code (remote).	9.8	More Details
CVE-2022-32054	Tenda AC10 US_AC10V1.0RTL_V15.03.06.26_multi_TD01 was discovered to contain a remote code execution (RCE) vulnerability via the lanIp parameter.	9.8	More Details
CVE-2022-33980	Apache Commons Configuration performs variable interpolation, allowing properties to be dynamically evaluated and expanded. The standard format for interpolation is "${prefix:name}", where "prefix" is used to locate an instance of org.apache.commons.configuration2.interpol.Lookup that performs the interpolation. Starting with version 2.4 and continuing through 2.7, the set of default Lookup instances included interpolators that could result in arbitrary code execution or contact with remote servers. These lookups are: - "script" - execute expressions using the JVM script execution engine (javax.script) - "dns" - resolve dns records - "url" - load values from urls, including from remote servers Applications using the interpolation defaults in the affected versions may be vulnerable to remote code execution or unintentional contact with remote servers if untrusted configuration values are used. Users are recommended to upgrade to Apache Commons Configuration 2.8.0, which disables the problematic interpolators by default.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26649	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.2), SCALANCE X201-3P IRT (All versions < V5.5.2), SCALANCE X201-3P IRT PRO (All versions < V5.5.2), SCALANCE X202-2IRT (All versions < V5.5.2), SCALANCE X202-2IRT (All versions < V5.5.2), SCALANCE X202-2P IRT (All versions < V5.5.2), SCALANCE X202-2P IRT PRO (All versions < V5.5.2), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions < V5.5.2), SCALANCE X204IRT (All versions < V5.5.2), SCALANCE X204IRT PRO (All versions < V5.5.2), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions < V5.5.2), SCALANCE XF202-2P IRT (All versions < V5.5.2), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions < V5.5.2), SCALANCE XF204IRT (All versions < V5.5.2), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.	9.6	More Details
CVE-2022-31557	The seveas/golem repository through 2016-05-17 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31563	The whmacmac/vprj repository through 2022-04-06 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31562	The waveyan/internshipsystem repository through 2018-05-22 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31561	The varijkapil13/Sphere_ImageBackend repository through 2019-10-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31560	The uncleYiba/photo_tag repository through 2020-08-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31559	The tsileo/flask-yeoman repository through 2013-09-13 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31558	The tooxie/shiva-server repository through 0.10.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31554	The rohitnayak/movie-review-sentiment-analysis repository through 2017-05-07 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31556	The rusyasoft/TrainEnergyServer repository through 2017-08-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31555	The romain20100/nursequest repository through 2018-02-22 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31565	The yogson/syrabond repository through 2020-05-25 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31553	The rainsoupah/sleep-learner repository through 2021-02-21 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31552	The project-anuvaad/anuvaad-corpus repository through 2020-11-23 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31551	The pleomax00/flask-mongo-skel repository through 2012-11-01 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31550	The olmax99/pyathenastack repository through 2019-11-08 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31549	The olmax99/helm-flask-celery repository before 2022-05-25 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31548	The nrlakin/homepage repository through 2017-03-06 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31564	The woduq1414/munhak-moa repository before 2022-05-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31571	The akashtalole/python-flask-restful-api repository through 2019-09-16 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31567	The DSABenchmark/DSAB repository through 2.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31581	The scorelab/OpenMF repository before 2022-05-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31588	The zippies/testplatform repository through 2016-07-19 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31587	The yuriyouzhou/KG-fashion-chatbot repository through 2018-05-22 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31586	The unizar-30226-2019-06/ChangePop-Back repository through 2019-06-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31585	The umeshpatil-dev/Home__internet repository through 2020-08-28 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31584	The stonethree/s3label repository through 2019-08-14 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31583	The sravaniboinepelli/AutomatedQuizEval repository through 2020-04-27 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31582	The shaolo1/VideoServer repository through 2019-09-21 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31580	The sanojtharindu/caretakerr-api repository through 2021-05-17 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31568	The Rexians/rex-web repository through 2022-06-05 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31579	The ralphjzhang/iasset repository through 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31577	The longmaoteamtf/audio_aligner_app repository through 2020-01-10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31576	The heidi-luong1109/shackerpanel repository through 2021-05-25 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31547	The noamezekiel/sphere repository through 2020-05-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31574	The deepaliupadhyay/RealEstate repository through 2018-11-30 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31573	The chainer/chainerrl-visualizer repository through 0.1.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31572	The ceee-vip/cockybook repository through 2015-04-16 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31575	The duducosmos/livro_python repository through 2018-06-06 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31546	The nlpweb/glance repository through 2014-06-27 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31545	The ml-inory/ModelConverter repository through 2021-04-26 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31511	The AFDudley/equanimity repository through 2014-04-23 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31520	The Luxas98/logstash-management-api repository through 2020-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31544	The meerstein/rbtm repository through 1.5 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31518	The JustAnotherSoftwareDeveloper/Python-Recipe-Database repository through 2021-03-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31517	The HolgerGraef/MSM repository through 2021-04-20 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31516	The Harveyzyh/Python repository through 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31515	The Delor4/CarceresBE repository through 1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31514	The Caoyongqi912/Fan_Platform repository through 2021-04-20 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31513	The BolunHan/Krypton repository through 2021-06-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31512	The Atom02/flask-mvc repository through 2020-09-14 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31510	The sergeKashkin/Simple-RAT repository before 2022-05-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31522	The NotVinay/karaokey repository through 2019-12-11 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31509	The iedadata/usap-dc-website repository through 1.0.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31508	The idayrus/evoting repository before 2022-05-08 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31507	The ganga-devs/ganga repository before 8.5.10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31506	The cmusatyalab/opendiamond repository through 10.1.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31505	The cheo0/MercadoEnLineaBack repository through 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31504	The ChangeWeDer/BaiduWenkuSpider_flaskWeb repository before 2021-11-29 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31503	The orchest/orchest repository before 2022.05.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31502	The operatorequals/wormnest repository through 0.4.7 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31501	The ChaoticOnyx/OnyxForum repository before 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31521	The Niyaz-Mohamed/mosaic repository through 1.0.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31519	The Lukasavicus/WindMill repository through 1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31523	The PaddlePaddle/Anakin repository through 0.1.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31535	The freefood89/Fishtank repository through 2015-06-24 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31543	The maxtortime/SetupBox repository through 1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31542	The mandoku/mdweb repository through 2015-05-07 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31541	The lyubolp/Barry-Voice-Assistant repository through 2021-01-18 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31540	The kumardeepak/hin-eng-preprocessing repository through 2019-07-16 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31539	The kotekan/kotekan repository through 2021.11 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31538	The joaopedro-fg/mp-m08-interface repository through 2020-12-10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31524	The PureStorage-OpenConnect/swagger repository through 1.1.5 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31536	The jaygarza1982/ytdl-sync repository through 2021-01-02 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31537	The jmcginty15/Solar-system-simulator repository through 2021-07-26 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31534	The echoleegroup/PythonWeb repository through 2018-10-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31532	The dankolbman/travel_blahg repository through 2016-01-16 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31531	The dainst/cilantro repository through 0.0.4 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31530	The csm-aut/csm repository through 3.5 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31529	The cinemaproject/monorepo repository through 2021-03-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31528	The bonn-activity-maps/bam_annotation_tool repository through 2021-08-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31527	The Wildog/flask-file-server repository through 2020-02-20 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31533	The decentraminds/umbral repository through 2020-01-15 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31526	The ThundeRatz/ThunderDocs repository through 2020-05-01 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-31525	The SummaLabs/DLS repository through 0.1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	9.3	More Details
CVE-2022-34737	The application security module has a vulnerability in permission assignment. Successful exploitation of this vulnerability may affect data integrity and confidentiality.	9.1	More Details
CVE-2021-46825	Symantec Advanced Secure Gateway (ASG) and ProxySG are susceptible to an HTTP desync vulnerability. When a remote unauthenticated attacker and other web clients communicate through the proxy with the same web server, the attacker can send crafted HTTP requests and cause the proxy to forward web server responses to unintended clients. Severity/CVSSv3: High / 8.1 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N	9.1	More Details
CVE-2014-8164	A insecure configuration for certificate verification (http.verify_mode = OpenSSL::SSL::VERIFY_NONE) may lead to verification bypass in Red Hat CloudForms 5.x.	9.1	More Details
CVE-2021-44222	A vulnerability has been identified in SIMATIC eaSie Core Package (All versions < V22.00). The underlying MQTT service of affected systems does not perform authentication in the default configuration. This could allow an unauthenticated remote attacker to send arbitrary messages to the service and thereby issue arbitrary requests in the affected system.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35169	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.5.2, contain an Improper Input Validation Vulnerability.	9.1	More Details
CVE-2022-20812	Multiple vulnerabilities in the API and in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow a remote attacker to overwrite arbitrary files or conduct null byte poisoning attacks on an affected device. Note: Cisco Expressway Series refers to the Expressway Control (Expressway-C) device and the Expressway Edge (Expressway-E) device. For more information about these vulnerabilities, see the Details section of this advisory.	9.0	More Details
CVE-2022-20813	Multiple vulnerabilities in the API and in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow a remote attacker to overwrite arbitrary files or conduct null byte poisoning attacks on an affected device. Note: Cisco Expressway Series refers to the Expressway Control (Expressway-C) device and the Expressway Edge (Expressway-E) device. For more information about these vulnerabilities, see the Details section of this advisory.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-33011	Known v1.3.1+2020120201 was discovered to allow attackers to perform an account takeover via a host header injection attack.	8.8	More Details
CVE-2021-38289	An issue has been discovered in Novastar-VNNOX-iCare Novaicare 7.16.0 that gives attacker privilege escalation and allows attackers to view corporate information and SMTP server details, delete users, view roles, and other unspecified impacts.	8.8	More Details
CVE-2022-35228	SAP BusinessObjects CMC allows an unauthenticated attacker to retrieve token information over the network which would otherwise be restricted. This can be achieved only when a legitimate user accesses the application and a local compromise occurs, like sniffing or social engineering. On successful exploitation, the attacker can completely compromise the application.	8.8	More Details
CVE-2022-31593	SAP Business One client - version 10.0 allows an attacker with low privileges, to inject code that can be executed by the application. An attacker could thereby control the behavior of the application.	8.8	More Details
CVE-2022-30929	Mini-Tmall v1.0 is vulnerable to Insecure Permissions via tomcat-embed-jasper.	8.8	More Details
CVE-2022-1025	All unpatched versions of Argo CD starting with v1.0.0 are vulnerable to an improper access control bug, allowing a malicious user to potentially escalate their privileges to admin-level.	8.8	More Details
CVE-2022-21768	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351.	8.8	More Details
CVE-2022-21767	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430.	8.8	More Details
CVE-2022-25048	Command injection vulnerability in CWP v0.9.8.1126 that allows normal users to run commands as the root user.	8.8	More Details
CVE-2022-33996	Incorrect permission management in Devolutions Server before 2022.2 allows a new user with a preexisting username to inherit the permissions of that previous user.	8.8	More Details
CVE-2022-22026	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability	8.8	More Details
CVE-2015-1784	In nextgen-galery wordpress plugin before 2.0.77.3 there are two vulnerabilities which can allow an attacker to gain full access over the web application. The vulnerabilities lie in how the application validates user uploaded files and lack of security measures preventing unwanted HTTP requests.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31138	mailcow is a mailserver suite. Prior to mailcow-dockerized version 2022-06a, an extended privilege vulnerability can be exploited by manipulating the custom parameters regexmess, skipmess, regexflag, delete2foldersonly, delete2foldersbutnot, regextrans2, pipemess, or maxlinelengthcmd to execute arbitrary code. Users should update their mailcow instances with the `update.sh` script in the mailcow root directory to 2022-06a or newer to receive a patch for this issue. As a temporary workaround, the Syncjob ACL can be removed from all mailbox users, preventing changes to those settings.	8.8	More Details
CVE-2022-30216	Windows Server Service Tampering Vulnerability	8.8	More Details
CVE-2022-26647	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.2), SCALANCE X201-3P IRT (All versions < V5.5.2), SCALANCE X201-3P IRT PRO (All versions < V5.5.2), SCALANCE X202-2IRT (All versions < V5.5.2), SCALANCE X202-2IRT (All versions < V5.5.2), SCALANCE X202-2P IRT (All versions < V5.5.2), SCALANCE X202-2P IRT PRO (All versions < V5.5.2), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions < V5.5.2), SCALANCE X204IRT (All versions < V5.5.2), SCALANCE X204IRT PRO (All versions < V5.5.2), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions < V5.5.2), SCALANCE XF202-2P IRT (All versions < V5.5.2), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions < V5.5.2), SCALANCE XF204IRT (All versions < V5.5.2), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions.	8.8	More Details
CVE-2022-30221	Windows Graphics Component Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-22476	IBM WebSphere Application Server Liberty 17.0.0.3 through 22.0.0.7 and Open Liberty are vulnerable to identity spoofing by an authenticated user using a specially crafted request. IBM X-Force ID: 225604.	8.8	More Details
CVE-2022-35414	softmmu/physmem.c in QEMU through 7.0.0 can perform an uninitialized read on the translate_fail path, leading to an io_readx or io_writex crash. NOTE: a third party states that the Non-virtualization Use Case in the qemu.org reference applies here, i.e., "Bugs affecting the non-virtualization use case are not considered security bugs at this time.	8.8	More Details
CVE-2022-31566	The DSAB-local/DSAB repository through 2019-02-18 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	8.6	More Details
CVE-2022-30754	Implicit Intent hijacking vulnerability in AppLinker prior to SMR Jul-2022 Release 1 allow allows attackers to launch certain activities with privilege of AppLinker.	8.5	More Details
CVE-2022-30756	Implicit Intent hijacking vulnerability in Finder prior to SMR Jul-2022 Release 1 allow allows attackers to launch certain activities with privilege of Finder.	8.5	More Details
CVE-2022-33703	Improper validation vulnerability in CACertificateInfo prior to SMR Jul-2022 Release 1 allows attackers to launch certain activities.	8.5	More Details
CVE-2022-33704	Improper validation vulnerability in ucmRetParcelable of KnoxSDK prior to SMR Jul-2022 Release 1 allows attackers to launch certain activities.	8.5	More Details
CVE-2022-34820	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions < V3.3.46), SIMATIC CP 1243-1 (All versions < V3.3.46), SIMATIC CP 1243-7 LTE EU (All versions < V3.3.46), SIMATIC CP 1243-7 LTE US (All versions < V3.3.46), SIMATIC CP 1243-8 IRC (All versions < V3.3.46), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0 < V2.2.28), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0 < V2.2.28), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0 < V2.2.28), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0 < V2.2.28), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0 < V2.2.28), SIPLUS NET CP 1242-7 V2 (All versions < V3.3.46), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions < V3.3.46), SIPLUS S7-1200 CP 1243-1 RAIL (All versions < V3.3.46). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30222	Windows Shell Remote Code Execution Vulnerability	8.4	More Details
CVE-2022-33674	Azure Site Recovery Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-31105	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Argo CD starting with version 0.4.0 and prior to 2.2.11, 2.3.6, and 2.4.5 is vulnerable to an improper certificate validation bug which could cause Argo CD to trust a malicious (or otherwise untrustworthy) OpenID Connect (OIDC) provider. A patch for this vulnerability has been released in Argo CD versions 2.4.5, 2.3.6, and 2.2.11. There are no complete workarounds, but a partial workaround is available. Those who use an external OIDC provider (not the bundled Dex instance), can mitigate the issue by setting the `oidc.config.rootCA` field in the `argocd-cm` ConfigMap. This mitigation only forces certificate validation when the API server handles login flows. It does not force certificate verification when verifying tokens on API calls.	8.3	More Details
CVE-2022-33680	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-26348	Command Centre Server is vulnerable to SQL Injection via Windows Registry settings for date fields on the server. The Windows Registry setting allows an attacker using the Visitor Management Kiosk, an application designed for public use, to invoke an arbitrary SQL query that has been preloaded into the registry of the Windows Server to obtain sensitive information. This issue affects: Gallagher Command Centre 8.60 versions prior to 8.60.1652; 8.50 versions prior to 8.50.2245; 8.40 versions prior to 8.40.2216; 8.30 versions prior to 8.30.1470; version 8.20 and prior versions.	8.2	More Details
CVE-2022-31012	Git for Windows is a fork of Git that contains Windows-specific patches. This vulnerability in versions prior to 2.37.1 lets Git for Windows' installer execute a binary into `C:\mingw64\bin\git.exe` by mistake. This only happens upon a fresh install, not when upgrading Git for Windows. A patch is included in version 2.37.1. Two workarounds are available. Create the `C:\mingw64` folder and remove read/write access from this folder, or disallow arbitrary authenticated users to create folders in `C:\`.	8.2	More Details
CVE-2022-26648	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.2), SCALANCE X201-3P IRT (All versions < V5.5.2), SCALANCE X201-3P IRT PRO (All versions < V5.5.2), SCALANCE X202-2IRT (All versions < V5.5.2), SCALANCE X202-2IRT (All versions < V5.5.2), SCALANCE X202-2P IRT (All versions < V5.5.2), SCALANCE X202-2P IRT PRO (All versions < V5.5.2), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions < V5.5.2), SCALANCE X204IRT (All versions < V5.5.2), SCALANCE X204IRT PRO (All versions < V5.5.2), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions < V5.5.2), SCALANCE XF202-2P IRT (All versions < V5.5.2), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions < V5.5.2), SCALANCE XF204IRT (All versions < V5.5.2), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices.	8.2	More Details
CVE-2022-24800	October/System is the system module for October CMS, a self-hosted CMS platform based on the Laravel PHP Framework. Prior to versions 1.0.476, 1.1.12, and 2.2.15, when the developer allows the user to specify their own filename in the `fromData` method, an unauthenticated user can perform remote code execution (RCE) by exploiting a race condition in the temporary storage directory. This vulnerability affects plugins that expose the `October\Rain\Database\Attach\File::fromData` as a public interface and does not affect vanilla installations of October CMS since this method is not exposed or used by the system internally or externally. The issue has been patched in Build 476 (v1.0.476), v1.1.12, and v2.2.15. Those who are unable to upgrade may apply with patch to their installation manually as a workaround.	8.1	More Details
CVE-2022-2385	A security issue was discovered in aws-iam-authenticator where an allow-listed IAM identity may be able to modify their username and escalate privileges.	8.1	More Details
CVE-2022-30602	Operation restriction bypass in multiple applications of Cybozu Garoon 4.0.0 to 5.9.1 allows a remote authenticated attacker to alter the file information and/or delete the files.	8.1	More Details
CVE-2022-22681	Session fixation vulnerability in access control management in Synology Photo Station before 6.8.16-3506 allows remote attackers to bypass security constraint via unspecified vectors.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22029	Windows Network File System Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-22038	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-33137	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions.	8.0	More Details
CVE-2022-33936	Cloud Mobility for Dell EMC Storage, 1.3.0.XXX contains a RCE vulnerability. A non-privileged user could potentially exploit this vulnerability, leading to achieving a root shell. This is a critical issue; so Dell recommends customers to upgrade at the earliest opportunity.	8.0	More Details
CVE-2022-22998	Implemented protections on AWS credentials that were not properly protected.	8.0	More Details
CVE-2022-34663	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100F, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200F, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969F, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM RS416NC, RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416P, RUGGEDCOM RS416PF, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNCv2 V4.X, RUGGEDCOM RS416PNCv2 V5.X, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300F, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488F, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. Affected devices are vulnerable to a web-based code injection attack via the console. An attacker could exploit this vulnerability to inject code into the web server and cause malicious behavior in legitimate users accessing certain web resources on the affected device.	8.0	More Details
CVE-2022-34748	A vulnerability has been identified in Simcenter Femap (All versions < V2022.2). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17293)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34281	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current process. (FG-VD-22-046)	7.8	More Details
CVE-2022-34284	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-049)	7.8	More Details
CVE-2022-34286	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-051)	7.8	More Details
CVE-2022-34289	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-054)	7.8	More Details
CVE-2022-34465	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.264), Parasolid V34.0 (All versions < V34.0.250), Parasolid V34.1 (All versions < V34.1.233), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds read past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15420)	7.8	More Details
CVE-2022-22027	Windows Fax Service Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-34279	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current process. (FG-VD-22-044)	7.8	More Details
CVE-2022-24139	In IOBit Advanced System Care (AscService.exe) 15, an attacker with SEImpersonatePrivilege can create a named pipe with the same name as one of ASCService's named pipes. ASCService first tries to connect before trying to create the named pipes, because of that during login the service will try to connect to the attacker which will lead to either escalation of privileges (through token manipulation and ImpersonateNamedPipeClient()) from ADMIN -> SYSTEM or from Local ADMIN -> Domain ADMIN depending on the user and named pipe that is used.	7.8	More Details
CVE-2021-36665	An issue was discovered in Druva 6.9.0 for macOS, allows attackers to gain escalated local privileges via the inSyncUpgradeDaemon.	7.8	More Details
CVE-2021-36666	An issue was discovered in Druva 6.9.0 for MacOS, allows attackers to gain escalated local privileges via the inSyncDecommission.	7.8	More Details
CVE-2021-36668	URL injection in Driva inSync 6.9.0 for MacOS, allows attackers to force a visit to an arbitrary url via the port parameter to the Electron App.	7.8	More Details
CVE-2022-30206	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-22050	Windows Fax Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-22049	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-34280	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current process. (FG-VD-22-045)	7.8	More Details
CVE-2022-34276	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-041)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34278	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-043)	7.8	More Details
CVE-2022-34277	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-042)	7.8	More Details
CVE-2022-22045	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-34275	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-040)	7.8	More Details
CVE-2022-34274	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-039)	7.8	More Details
CVE-2022-34273	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-038)	7.8	More Details
CVE-2022-24138	IOBit Advanced System Care (Asc.exe) 15 and Action Download Center both download components of IOBit suite into ProgramData folder, ProgramData folder has "rwx" permissions for unprivileged users. Low privilege users can use SetOpLock to wait for CreateProcess and switch the genuine component with a malicious executable thus gaining code execution as a high privilege user (Low Privilege -> high integrity ADMIN).	7.8	More Details
CVE-2022-34272	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current process. (FG-VD-22-037, FG-VD-22-059)	7.8	More Details
CVE-2022-30220	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-33675	Azure Site Recovery Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-2345	Use After Free in GitHub repository vim/vim prior to 9.0.0046.	7.8	More Details
CVE-2022-32481	Dell PowerProtect Cyber Recovery, versions prior to 19.11, contain a privilege escalation vulnerability on virtual appliance deployments. A lower-privileged authenticated user can chain docker commands to escalate privileges to root leading to complete system takeover.	7.8	More Details
CVE-2022-2344	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0045.	7.8	More Details
CVE-2022-2343	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0044.	7.8	More Details
CVE-2022-22465	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 could allow a local user to obtain elevated privileges due to improper access permissions. IBM X-Force ID: 225082.	7.8	More Details
CVE-2022-22047	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36667	Command injection vulnerability in Druva inSync 6.9.0 for MacOS, allows attackers to execute arbitrary commands via crafted payload to the local HTTP server due to un-sanitized call to the python os.system library.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33708	Improper input validation vulnerability in AppsPackageInstaller in Galaxy Store prior to version 4.5.41.8 allows local attackers to launch activities as Galaxy Store privilege.	7.8	More Details
CVE-2022-22043	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-22024	Windows Fax Service Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21777	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894.	7.8	More Details
CVE-2022-22031	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-31591	SAP BusinessObjects BW Publisher Service - versions 420, 430, uses a search path that contains an unquoted element. A local attacker can gain elevated privileges by inserting an executable file in the path of the affected service	7.8	More Details
CVE-2022-22034	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-23714	A local privilege escalation (LPE) issue was discovered in the ransomware canaries features of Elastic Endpoint Security for Windows, which could allow unprivileged users to elevate their privileges to those of the LocalSystem account.	7.8	More Details
CVE-2022-29187	Git is a distributed revision control system. Git prior to versions 2.37.1, 2.36.2, 2.35.4, 2.34.4, 2.33.4, 2.32.3, 2.31.4, and 2.30.5, is vulnerable to privilege escalation in all platforms. An unsuspecting user could still be affected by the issue reported in CVE-2022-24765, for example when navigating as root into a shared tmp directory that is owned by them, but where an attacker could create a git repository. Versions 2.37.1, 2.36.2, 2.35.4, 2.34.4, 2.33.4, 2.32.3, 2.31.4, and 2.30.5 contain a patch for this issue. The simplest way to avoid being affected by the exploit described in the example is to avoid running git as root (or an Administrator in Windows), and if needed to reduce its use to a minimum. While a generic workaround is not possible, a system could be hardened from the exploit described in the example by removing any such repository if it exists already and creating one as root to block any future attacks.	7.8	More Details
CVE-2022-33709	Improper input validation vulnerability in ApexPackageInstaller in Galaxy Store prior to version 4.5.41.8 allows local attackers to launch activities as Galaxy Store privilege.	7.8	More Details
CVE-2022-33710	Improper input validation vulnerability in BillingPackageInsraller in Galaxy Store prior to version 4.5.41.8 allows local attackers to launch activities as Galaxy Store privilege.	7.8	More Details
CVE-2022-20808	A vulnerability in Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to incorrect handling of multiple simultaneous device registrations on Cisco SSM On-Prem. An attacker could exploit this vulnerability by sending multiple device registration requests to Cisco SSM On-Prem. A successful exploit could allow the attacker to cause a DoS condition on an affected device.	7.7	More Details
CVE-2022-31124	openssh_key_parser is an open source Python package providing utilities to parse and pack OpenSSH private and public key files. In versions prior to 0.0.6 if a field of a key is shorter than it is declared to be, the parser raises an error with a message containing the raw field value. An attacker able to modify the declared length of a key's sensitive field can thus expose the raw value of that field. Users are advised to upgrade to version 0.0.6, which no longer includes the raw field value in the error message. There are no known workarounds for this issue.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34821	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.2), SCALANCE M804PB (All versions < V7.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.2), SCALANCE M874-2 (All versions < V7.2), SCALANCE M874-3 (All versions < V7.2), SCALANCE M876-3 (EVDO) (All versions < V7.2), SCALANCE M876-3 (ROK) (All versions < V7.2), SCALANCE M876-4 (All versions < V7.2), SCALANCE M876-4 (EU) (All versions < V7.2), SCALANCE M876-4 (NAM) (All versions < V7.2), SCALANCE MUM853-1 (EU) (All versions < V7.2), SCALANCE MUM856-1 (EU) (All versions < V7.2), SCALANCE MUM856-1 (RoW) (All versions < V7.2), SCALANCE S615 (All versions < V7.2), SCALANCE S615 EEC (All versions < V7.2), SCALANCE SC622-2C (All versions < V2.3), SCALANCE SC622-2C (All versions >= V2.3 < V3.0), SCALANCE SC626-2C (All versions < V2.3), SCALANCE SC626-2C (All versions >= V2.3 < V3.0), SCALANCE SC632-2C (All versions < V2.3), SCALANCE SC632-2C (All versions >= V2.3 < V3.0), SCALANCE SC636-2C (All versions < V2.3), SCALANCE SC636-2C (All versions >= V2.3 < V3.0), SCALANCE SC642-2C (All versions < V2.3), SCALANCE SC642-2C (All versions >= V2.3 < V3.0), SCALANCE SC646-2C (All versions < V2.3), SCALANCE SC646-2C (All versions >= V2.3 < V3.0), SCALANCE WAM763-1 (All versions), SCALANCE WAM766-1 (EU) (All versions), SCALANCE WAM766-1 (US) (All versions), SCALANCE WAM766-1 EEC (EU) (All versions), SCALANCE WAM766-1 EEC (US) (All versions), SCALANCE WUM763-1 (All versions), SCALANCE WUM763-1 (All versions), SCALANCE WUM766-1 (EU) (All versions), SCALANCE WUM766-1 (US) (All versions), SIMATIC CP 1242-7 V2 (All versions < V3.3.46), SIMATIC CP 1243-1 (All versions < V3.3.46), SIMATIC CP 1243-7 LTE EU (All versions < V3.3.46), SIMATIC CP 1243-7 LTE US (All versions < V3.3.46), SIMATIC CP 1243-8 IRC (All versions < V3.3.46), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0 < V2.2.28), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0 < V2.2.28), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0 < V2.2.28), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0 < V2.2.28), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0 < V2.2.28), SIPLUS NET CP 1242-7 V2 (All versions < V3.3.46), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions < V3.3.46), SIPLUS S7-1200 CP 1243-1 RAIL (All versions < V3.3.46). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges.	7.6	More Details
CVE-2021-46741	The basic framework and setting module have defects, which were introduced during the design. Successful exploitation of this vulnerability may affect system integrity.	7.5	More Details
CVE-2022-30792	In CmpChannelServer of CODESYS V3 in multiple versions an uncontrolled ressource consumption allows an unauthorized attacker to block new communication channel connections. Existing connections are not affected.	7.5	More Details
CVE-2021-41396	Live555 through 1.08 does not handle socket connections properly. A huge number of incoming socket connections in a short time invokes the error-handling module, in which a heap-based buffer overflow happens. An attacker can leverage this to launch a DoS attack.	7.5	More Details
CVE-2022-33736	A vulnerability has been identified in Opcenter Quality V13.1 (All versions < V13.1.20220624), Opcenter Quality V13.2 (All versions < V13.2.20220624). The affected applications do not properly validate login information during authentication. This could lead to denial of service condition for existing users or allow unauthenticated remote attackers to successfully login without credentials.	7.5	More Details
CVE-2022-33138	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device.	7.5	More Details
CVE-2022-31257	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.31), Mendix Applications using Mendix 8 (All versions < V8.18.18), Mendix Applications using Mendix 9 (All versions < V9.14.0), Mendix Applications using Mendix 9 (V9.12) (All versions < V9.12.2), Mendix Applications using Mendix 9 (V9.6) (All versions < V9.6.12). In case of access to an active user session in an application that is built with an affected version, it's possible to change that user's password bypassing password validations within a Mendix application. This could allow to set weak passwords.	7.5	More Details
CVE-2022-30938	A vulnerability has been identified in EN100 Ethernet module DNP3 IP variant (All versions), EN100 Ethernet module IEC 104 variant (All versions), EN100 Ethernet module IEC 61850 variant (All versions < V4.40), EN100 Ethernet module Modbus TCP variant (All versions), EN100 Ethernet module PROFINET IO variant (All versions). Affected applications contains a memory corruption vulnerability while parsing specially crafted HTTP packets to /txtrace endpoint manupulating a specific argument. This could allow an attacker to crash the affected application leading to a denial of service condition	7.5	More Details
CVE-2022-29884	A vulnerability has been identified in CP-8000 MASTER MODULE WITH I/O -25/+70°C (All versions < CPC80 V16.30), CP-8000 MASTER MODULE WITH I/O -40/+70°C (All versions < CPC80 V16.30), CP-8021 MASTER MODULE (All versions < CPC80 V16.30), CP-8022 MASTER MODULE WITH GPRS (All versions < CPC80 V16.30). When using the HTTPS server under specific conditions, affected devices do not properly free resources. This could allow an unauthenticated remote attacker to put the device into a denial of service condition.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30215	Active Directory Federation Services Elevation of Privilege Vulnerability	7.5	More Details
CVE-2021-44221	A vulnerability has been identified in SIMATIC eaSie Core Package (All versions < V22.00). The affected systems do not properly validate input that is sent to the underlying message passing framework. This could allow an remote attacker to trigger a denial of service of the affected system.	7.5	More Details
CVE-2022-31140	Valinor is a PHP library that helps to map any input into a strongly-typed value object structure. Prior to version 0.12.0, Valinor can use `Throwable#getMessage()` when it should not have permission to do so. This is a problem with cases such as an SQL exception showing an SQL snippet, a database connection exception showing database IP address/username/password, or a timeout detail / out of memory detail. Attackers could use this information for potential data exfiltration, denial of service attacks, enumeration attacks, etc. Version 0.12.0 contains a patch for this vulnerability.	7.5	More Details
CVE-2022-30591	quic-go through 0.27.0 allows remote attackers to cause a denial of service (CPU consumption) via a Slowloris variant in which incomplete QUIC or HTTP/3 requests are sent. This occurs because mtu_discoverer.go misparses the MTU Discovery service and consequently overflows the probe timer. NOTE: the vendor's position is that this behavior should not be listed as a vulnerability on the CVE List	7.5	More Details
CVE-2022-30791	In CmpBlkDrvTcp of CODESYS V3 in multiple versions an uncontrolled ressource consumption allows an unauthorized attacker to block new TCP connections. Existing connections are not affected.	7.5	More Details
CVE-2022-32058	An infinite loop in the function httpRpmPass of TP-Link TL-WR741N/TL-WR742N V1/V2/V3_130415 allows attackers to cause a Denial of Service (DoS) via a crafted packet.	7.5	More Details
CVE-2022-31578	The piaoyunsoft/bt_lnmp repository through 2019-10-10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	7.5	More Details
CVE-2022-33713	Implicit Intent hijacking vulnerability in Samsung Cloud prior to version 5.2.0 allows attacker to get sensitive information.	7.5	More Details
CVE-2022-2048	In Eclipse Jetty HTTP/2 server implementation, when encountering an invalid HTTP/2 request, the error handling has a bug that can wind up not properly cleaning up the active connections and associated resources. This can lead to a Denial of Service scenario where there are no enough resources left to process good requests.	7.5	More Details
CVE-2022-2191	In Eclipse Jetty versions 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, SslConnection does not release ByteBuffers from configured ByteBufferPool in case of error code paths.	7.5	More Details
CVE-2022-32249	Under special integration scenario of SAP Business one and SAP HANA - version 10.0, an attacker can exploit HANA cockpit&#65533;s data volume to gain access to highly sensitive information (e.g., high privileged account credentials)	7.5	More Details
CVE-2022-35168	Due to improper input sanitization of XML input in SAP Business One - version 10.0, an attacker can perform a denial-of-service attack rendering the system temporarily inoperative.	7.5	More Details
CVE-2022-33173	An algorithm-downgrade issue was discovered in Couchbase Server before 7.0.4. Analytics Remote Links may temporarily downgrade to non-TLS connection to determine the TLS port number, using SCRAM-SHA instead.	7.5	More Details
CVE-2022-35410	mat2 (aka metadata anonymisation toolkit) before 0.13.0 allows ../ directory traversal during the ZIP archive cleaning process. This primarily affects mat2 web instances, in which clients could obtain sensitive information via a crafted archive.	7.5	More Details
CVE-2022-35403	Zoho ManageEngine ServiceDesk Plus before 13008, ServiceDesk Plus MSP before 10606, and SupportCenter Plus before 11022 are affected by an unauthenticated local file disclosure vulnerability via ticket-creation email. (This also affects Asset Explorer before 6977 with authentication.)	7.5	More Details
CVE-2022-22464	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 225081.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28771	Due to missing authentication check, SAP Business one License service API - version 10.0 allows an unauthenticated attacker to send malicious http requests over the network. On successful exploitation, an attacker can break the whole application making it inaccessible.	7.5	More Details
CVE-2022-22037	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	7.5	More Details
CVE-2022-32055	Inout Homestay v2.2 was discovered to contain a SQL injection vulnerability via the guests parameter at /index.php?page=search/rentals.	7.5	More Details
CVE-2020-4157	IBM QRadar Network Security 5.4.0 and 5.5.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174337.	7.5	More Details
CVE-2021-40012	Vulnerability of pointers being incorrectly used during data transmission in the video framework. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2021-39999	There is a buffer overflow vulnerability in eSE620X vESS V100R001C10SPC200 and V100R001C20SPC200. An attacker can exploit this vulnerability by sending a specific message to the target device due to insufficient validation of packets. Successful exploit could cause a denial of service condition.	7.5	More Details
CVE-2022-30211	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability	7.5	More Details
CVE-2022-34735	The frame scheduling module has a null pointer dereference vulnerability. Successful exploitation of this vulnerability will affect the kernel availability.	7.5	More Details
CVE-2022-22025	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability	7.5	More Details
CVE-2022-34736	The frame scheduling module has a null pointer dereference vulnerability. Successful exploitation of this vulnerability will affect the kernel availability.	7.5	More Details
CVE-2022-34738	The SystemUI module has a vulnerability in permission control. If this vulnerability is successfully exploited, users are unaware of the service running in the background.	7.5	More Details
CVE-2022-34739	The fingerprint module has a vulnerability of overflow in arithmetic addition. Successful exploitation of this vulnerability may result in the acquisition of data from unknown addresses in address mappings.	7.5	More Details
CVE-2021-4234	OpenVPN Access Server 2.10 and prior versions are susceptible to resending multiple packets in a response to a reset packet sent from the client which the client again does not respond to, resulting in a limited amplification attack.	7.5	More Details
CVE-2015-5236	It was discovered that the IcedTea-Web used codebase attribute of the <applet> tag on the HTML page that hosts Java applet in the Same Origin Policy (SOP) checks. As the specified codebase does not have to match the applet's actual origin, this allowed malicious site to bypass SOP via spoofed codebase value.	7.5	More Details
CVE-2022-34742	The system module has a read/write vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-34743	The AT commands of the USB port have an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may affect system availability.	7.5	More Details
CVE-2022-33737	The OpenVPN Access Server installer creates a log file readable for everyone, which from version 2.10.0 and before 2.11.0 may contain a random generated admin password	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33738	OpenVPN Access Server before 2.11 uses a weak random generator used to create user session token for the web portal	7.5	More Details
CVE-2020-4159	IBM QRadar Network Security 5.4.0 and 5.5.0 discloses sensitive information to unauthorized users which could be used to mount further attacks against the system. IBM X-Force ID: 174339.	7.5	More Details
CVE-2022-31129	moment is a JavaScript date library for parsing, validating, manipulating, and formatting dates. Affected versions of moment were found to use an inefficient parsing algorithm. Specifically using string-to-date parsing in moment (more specifically rfc2822 parsing, which is tried by default) has quadratic (N^2) complexity on specific inputs. Users may notice a noticeable slowdown is observed with inputs above 10k characters. Users who pass user-provided strings without sanity length checks to moment constructor are vulnerable to (Re)DoS attacks. The problem is patched in 2.29.4, the patch can be applied to all affected versions with minimal tweaking. Users are advised to upgrade. Users unable to upgrade should consider limiting date lengths accepted from user input.	7.5	More Details
CVE-2022-31121	Hyperledger Fabric is a permissioned distributed ledger framework. In affected versions if a consensus client sends a malformed consensus request to an orderer it may crash the orderer node. A fix has been added in commit 0f1835949 which checks for missing consensus messages and returns an error to the consensus client should the message be missing. Users are advised to upgrade to versions 2.2.7 or v2.4.5. There are no known workarounds for this issue.	7.5	More Details
CVE-2022-22039	Windows Network File System Remote Code Execution Vulnerability	7.5	More Details
CVE-2022-26078	Gallagher Controller 6000 is vulnerable to a Denial of Service attack via conflicting ARP packets with a duplicate IP address. This issue affects: Gallagher Gallagher Controller 6000 vCR8.60 versions prior to 220303a; vCR8.50 versions prior to 220303a; vCR8.40 versions prior to 220303a; vCR8.30 versions prior to 220303a.	7.5	More Details
CVE-2021-31645	An issue was discovered in glFTPd 2.11a that allows remote attackers to cause a denial of service via exceeding the connection limit.	7.5	More Details
CVE-2022-2339	With this SSRF vulnerability, an attacker can reach internal addresses to make a request as the server and read it's contents. This attack can lead to leak of sensitive information.	7.5	More Details
CVE-2022-30203	Windows Boot Manager Security Feature Bypass Vulnerability	7.4	More Details
CVE-2022-30209	Windows IIS Server Elevation of Privilege Vulnerability	7.4	More Details
CVE-2022-22040	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability	7.3	More Details
CVE-2022-30755	Improper authentication vulnerability in AppLock prior to SMR Jul-2022 Release 1 allows attacker to bypass password confirm activity by hijacking the implicit intent.	7.3	More Details
CVE-2022-2298	A vulnerability has been found in SourceCodester Clinics Patient Management System 2.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /pms/index.php of the component Login Page. The manipulation of the argument user_name with the input admin' or '1'='1 leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2022-33633	Skype for Business and Lync Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-33676	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29560	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < 2.15.1), RUGGEDCOM ROX MX5000RE (All versions < 2.15.1), RUGGEDCOM ROX RX1400 (All versions < 2.15.1), RUGGEDCOM ROX RX1500 (All versions < 2.15.1), RUGGEDCOM ROX RX1501 (All versions < 2.15.1), RUGGEDCOM ROX RX1510 (All versions < 2.15.1), RUGGEDCOM ROX RX1511 (All versions < 2.15.1), RUGGEDCOM ROX RX1512 (All versions < 2.15.1), RUGGEDCOM ROX RX1524 (All versions < 2.15.1), RUGGEDCOM ROX RX1536 (All versions < 2.15.1), RUGGEDCOM ROX RX5000 (All versions < 2.15.1). Affected devices do not properly validate user input, making them susceptible to command injection. An attacker with access to either the shell or the web CLI with administrator privileges could access the underlying operating system as the root user.	7.2	More Details
CVE-2022-33677	Azure Site Recovery Elevation of Privilege Vulnerability	7.2	More Details
CVE-2022-33678	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-31854	Codoforum v5.1 was discovered to contain an arbitrary file upload vulnerability via the logo change option in the admin panel.	7.2	More Details
CVE-2015-3173	custom-content-type-manager Wordpress plugin can be used by an administrator to achieve arbitrary PHP remote code execution.	7.2	More Details
CVE-2022-28935	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability.	7.2	More Details
CVE-2022-30225	Windows Media Player Network Sharing Service Elevation of Privilege Vulnerability	7.1	More Details
CVE-2020-29505	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.5.2, contain a Key Management Error Vulnerability.	7.1	More Details
CVE-2022-22022	Windows Print Spooler Elevation of Privilege Vulnerability	7.1	More Details
CVE-2022-30226	Windows Print Spooler Elevation of Privilege Vulnerability	7.1	More Details
CVE-2022-31127	NextAuth.js is a complete open source authentication solution for Next.js applications. An attacker can pass a compromised input to the e-mail [signin endpoint](https://next-auth.js.org/getting-started/rest-api#post-apiauthsigninprovider) that contains some malicious HTML, tricking the e-mail server to send it to the user, so they can perform a phishing attack. Eg.: `balazs@email.com, <a href="http://attacker.com">Before signing in, claim your money!</a>`. This was previously sent to `balazs@email.com`, and the content of the email containing a link to the attacker's site was rendered in the HTML. This has been remedied in the following releases, by simply not rendering that e-mail in the HTML, since it should be obvious to the receiver what e-mail they used: next-auth v3 users before version 3.29.8 are impacted. (We recommend upgrading to v4, as v3 is considered unmaintained. next-auth v4 users before version 4.9.0 are impacted. If for some reason you cannot upgrade, the workaround requires you to sanitize the `email` parameter that is passed to `sendVerificationRequest` and rendered in the HTML. If you haven't created a custom `sendVerificationRequest`, you only need to upgrade. Otherwise, make sure to either exclude `email` from the HTML body or efficiently sanitize it.	7.1	More Details
CVE-2022-33644	Xbox Live Save Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-22036	Performance Counters for Windows Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-30224	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3697	A crafted JPEG image may lead the JPEG reader to underflow its data pointer, allowing user-controlled data to be written in heap. To a successful to be performed the attacker needs to perform some triage over the heap layout and craft an image with a malicious format and payload. This vulnerability can lead to data corruption and eventual code execution or secure boot circumvention. This flaw affects grub2 versions prior grub-2.12.	7.0	More Details
CVE-2022-20082	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730.	7.0	More Details
CVE-2022-30202	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-22997	Addressed a remote code execution vulnerability by resolving a command injection vulnerability and closing an AWS S3 bucket that potentially allowed an attacker to execute unsigned code on My Cloud Home devices.	6.8	More Details
CVE-2020-29506	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.5.2, contain an Observable Timing Discrepancy Vulnerability.	6.8	More Details
CVE-2022-22041	Windows Print Spooler Elevation of Privilege Vulnerability	6.8	More Details
CVE-2022-21766	In CCCI, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641653.	6.7	More Details
CVE-2022-21773	In TEEI driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388.	6.7	More Details
CVE-2022-21765	In CCCI, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641673.	6.7	More Details
CVE-2022-21785	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06807363; Issue ID: ALPS06807363.	6.7	More Details
CVE-2020-35164	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.6, contain an Observable Timing Discrepancy Vulnerability.	6.7	More Details
CVE-2022-21787	In audio DSP, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558844; Issue ID: ALPS06558844.	6.7	More Details
CVE-2022-21770	In sound driver, there is a possible information disclosure due to symlink following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663.	6.7	More Details
CVE-2022-21771	In GED driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585.	6.7	More Details
CVE-2022-21772	In TEEI driver, there is a possible type confusion due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493842; Issue ID: ALPS06493842.	6.7	More Details
CVE-2022-21786	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822.	6.7	More Details
CVE-2022-21783	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704482.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21774	In TEEI driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641447; Issue ID: ALPS06641447.	6.7	More Details
CVE-2022-21775	In sched driver, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479032; Issue ID: ALPS06479032.	6.7	More Details
CVE-2022-21779	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704393.	6.7	More Details
CVE-2022-21780	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704526.	6.7	More Details
CVE-2022-21781	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704433.	6.7	More Details
CVE-2022-21782	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704508.	6.7	More Details
CVE-2022-21784	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704462.	6.7	More Details
CVE-2022-22023	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability	6.6	More Details
CVE-2022-30205	Windows Group Policy Elevation of Privilege Vulnerability	6.6	More Details
CVE-2022-30214	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2022-24140	IOBit Advanced System Care 15, iTop Screen Recorder 2.1, iTop VPN 3.2, Driver Booster 9, and iTop Screenshot sends HTTP requests in their update procedure in order to download a config file. After downloading the config file, the products will parse the HTTP location of the update from the file and will try to install the update automatically with ADMIN privileges. An attacker Intercepting this communication can supply the product a fake config file with malicious locations for the updates thus gaining a remote code execution on an endpoint.	6.6	More Details
CVE-2022-29900	Mis-trained branch predictions for return instructions may allow arbitrary speculative code execution under certain microarchitecture-dependent conditions.	6.5	More Details
CVE-2022-31073	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the ServiceBus server on the edge side may be susceptible to a DoS attack if an HTTP request containing a very large Body is sent to it. It is possible for the node to be exhausted of memory. The consequence of the exhaustion is that other services on the node, e.g. other containers, will be unable to allocate memory and thus causing a denial of service. Malicious apps accidentally pulled by users on the host and have the access to send HTTP requests to localhost may make an attack. It will be affected only when users enable the `ServiceBus` module in the config file `edgecore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the `ServiceBus` module in the config file `edgecore.yaml`.	6.5	More Details
CVE-2022-22682	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in Event Management in Synology Calendar before 2.4.5-10930 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	6.5	More Details
CVE-2021-31677	An issue was discovered in PESCMS-V2.3.3. There is a CSRF vulnerability that can modify admin and other members' passwords.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31678	An issue was discovered in PESCMS-V2.3.3. There is a CSRF vulnerability that can delete import information about a user's company.	6.5	More Details
CVE-2021-31679	An issue was discovered in PESCMS-V2.3.3. There is a CSRF vulnerability that allows attackers to delete admin and other members' account numbers.	6.5	More Details
CVE-2022-29619	Under certain conditions SAP BusinessObjects Business Intelligence Platform 4.x - versions 420,430 allows user Administrator to view, edit or modify rights of objects it doesn't own and which would otherwise be restricted.	6.5	More Details
CVE-2022-30208	Windows Security Account Manager (SAM) Denial of Service Vulnerability	6.5	More Details
CVE-2022-2091	The Cache Images WordPress plugin before 3.2.1 does not implement nonce checks, which could allow attackers to make any logged user upload images via a CSRF attack.	6.5	More Details
CVE-2022-20859	A vulnerability in the Disaster Recovery framework of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), and Cisco Unity Connection could allow an authenticated, remote attacker to perform certain administrative actions they should not be able to. This vulnerability is due to insufficient access control checks on the affected device. An attacker with read-only privileges could exploit this vulnerability by executing a specific vulnerable command on an affected device. A successful exploit could allow the attacker to perform a set of administrative actions they should not be able to.	6.5	More Details
CVE-2022-34741	The NFC module has a buffer overflow vulnerability. Successful exploitation of this vulnerability may cause exceptions in NFC card registration, deletion, and activation.	6.5	More Details
CVE-2015-5298	The Google Login Plugin (versions 1.0 and 1.1) allows malicious anonymous users to authenticate successfully against Jenkins instances that are supposed to be locked down to a particular Google Apps domain through client-side request modification.	6.5	More Details
CVE-2022-31135	Akashi is an open source server implementation of the Attorney Online video game based on the Ace Attorney universe. Affected versions of Akashi are subject to a denial of service attack. An attacker can use a specially crafted evidence packet to make an illegal modification, causing a server crash. This can be used to mount a denial-of-service exploit. Users are advised to upgrade. There is no known workaround for this issue.	6.5	More Details
CVE-2022-34740	The NFC module has a buffer overflow vulnerability. Successful exploitation of this vulnerability may cause exceptions in NFC card registration, deletion, and activation.	6.5	More Details
CVE-2022-30181	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-34466	A vulnerability has been identified in Mendix Applications using Mendix 9 (All versions >= V9.11 < V9.15), Mendix Applications using Mendix 9 (V9.12) (All versions < V9.12.3). An expression injection vulnerability was discovered in the Workflow subsystem of Mendix Runtime, that can affect the running applications. The vulnerability could allow a malicious user to leak sensitive information in a certain configuration.	6.5	More Details
CVE-2022-34467	A vulnerability has been identified in Mendix Excel Importer Module (Mendix 8 compatible) (All versions < V9.2.2), Mendix Excel Importer Module (Mendix 9 compatible) (All versions < V10.1.2). The affected component is vulnerable to XML Entity Expansion Injection. An attacker may use this to compromise the availability of the affected component.	6.5	More Details
CVE-2022-22042	Windows Hyper-V Information Disclosure Vulnerability	6.5	More Details
CVE-2022-32206	curl < 7.84.0 supports "chained" HTTP compression algorithms, meaning that a serverresponse can be compressed multiple times and potentially with different algorithms. The number of acceptable "links" in this "decompression chain" was unbounded, allowing a malicious server to insert a virtually unlimited number of compression steps.The use of such a decompression chain could result in a "malloc bomb", makingcurl end up spending enormous amounts of allocated heap memory, or trying toand returning out of memory errors.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40013	Improper permission control vulnerability in the Bluetooth module.Successful exploitation of this vulnerability will affect integrity.	6.5	More Details
CVE-2022-1732	The Rename wp-login.php WordPress plugin through 2.6.0 does not have CSRF check in place when updating the secret login URL, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2022-20791	A vulnerability in the database user privileges of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an authenticated, remote attacker to read arbitrary files on the underlying operating system of an affected device. This vulnerability is due to insufficient file permission restrictions. An attacker could exploit this vulnerability by sending a crafted command from the API to the application. A successful exploit could allow the attacker to read arbitrary files on the underlying operating system of the affected device. The attacker would need valid user credentials to exploit this vulnerability.	6.5	More Details
CVE-2015-1785	In nextgen-galery wordpress plugin before 2.0.77.3 there are two vulnerabilities which can allow an attacker to gain full access over the web application. The vulnerabilities lie in how the application validates user uploaded files and lack of security measures preventing unwanted HTTP requests.	6.5	More Details
CVE-2022-2211	A vulnerability was found in libguestfs. This issue occurs while calculating the greatest possible number of matching keys in the get_keys() function. This flaw leads to a denial of service, either by mistake or malicious actor.	6.5	More Details
CVE-2021-40016	Improper permission control vulnerability in the Bluetooth module.Successful exploitation of this vulnerability will affect confidentiality.	6.5	More Details
CVE-2022-33667	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-33663	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-33661	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-33672	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-2368	Authentication Bypass by Spoofing in GitHub repository microweber/microweber prior to 1.2.20.	6.5	More Details
CVE-2022-33657	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-33656	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-33637	Microsoft Defender for Endpoint Tampering Vulnerability	6.5	More Details
CVE-2022-33665	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-33641	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33655	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-33643	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-1576	The WP Maintenance Mode & Coming Soon WordPress plugin before 2.4.5 is lacking CSRF when emptying the subscribed users list, which could allow attackers to make a logged in admin perform such action via a CSRF attack	6.5	More Details
CVE-2022-1599	The Admin Management Xtended WordPress plugin before 2.4.5 does not have CSRF checks in some of its AJAX actions, allowing attackers to make a logged users with the right capabilities to call them. This can lead to changes in post status (draft, published), slug, post date, comment status (enabled, disabled) and more.	6.5	More Details
CVE-2022-29512	Exposure of sensitive information to an unauthorized actor issue in multiple applications of Cybozu Garoon 4.0.0 to 5.9.1 allows a remote authenticated attacker to obtain the data without the viewing privilege.	6.5	More Details
CVE-2022-33666	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-22463	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 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: 225079.	6.5	More Details
CVE-2022-33673	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-33662	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-21776	In MDP, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545450; Issue ID: ALPS06545450.	6.4	More Details
CVE-2022-31136	Bookwyrm is an open source social reading and reviewing program. Versions of Bookwyrm prior to 0.4.1 did not properly sanitize html being rendered to users. Unprivileged users are able to inject scripts into user profiles, book descriptions, and statuses. These vulnerabilities may be exploited as cross site scripting attacks on users viewing these fields. Users are advised to upgrade to version 0.4.1. There are no known workarounds for this issue.	6.3	More Details
CVE-2022-2297	A vulnerability, which was classified as critical, was found in SourceCodester Clinics Patient Management System 2.0. Affected is an unknown function of the file /pms/update_user.php?user_id=1. The manipulation of the argument profile_picture with the input <?php phpinfo();?> leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2022-33691	A possible race condition vulnerability in score driver prior to SMR Jul-2022 Release 1 can allow local attackers to interleave malicious operations.	6.2	More Details
CVE-2022-33689	Improper access control vulnerability in TelephonyUI prior to SMR Jul-2022 Release 1 allows attackers to change preferred network type by unprotected binder call.	6.2	More Details
CVE-2022-33702	Improper authorization vulnerability in Knoxguard prior to SMR Jul-2022 Release 1 allows local attacker to disable keyguard and bypass Knoxguard lock by factory reset.	6.2	More Details
CVE-2022-35227	A vulnerability in SAP NW EP (WPC) - versions 7.30, 7.31, 7.40, 7.50, which does not sufficiently validate user-controlled input, allows a remote attacker to conduct a Cross-Site (XSS) scripting attack. A successful exploit could allow the attacker to execute arbitrary script code which could lead to stealing or modifying of authentication information of the user, such as data relating to his or her current session.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1951	The core plugin for kitestudio WordPress plugin before 2.3.1 does not sanitise and escape some parameters before outputting them back in a response of an AJAX action, available to both unauthenticated and authenticated users when a premium theme from the vendor is active, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-2092	The WooCommerce PDF Invoices & Packing Slips WordPress plugin before 2.16.0 doesn't escape a parameter on its setting page, making it possible for attackers to conduct reflected cross-site scripting attacks.	6.1	More Details
CVE-2022-33098	Magnolia CMS v6.2.19 was discovered to contain a cross-site scripting (XSS) vulnerability via the Edit Contact function. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2022-1546	The WooCommerce - Product Importer WordPress plugin through 1.5.2 does not sanitise and escape the imported data before outputting it back in the page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-44791	In Apache Druid 0.22.1 and earlier, certain specially-crafted links result in unescaped URL parameters being sent back in HTML responses. This makes it possible to execute reflected XSS attacks.	6.1	More Details
CVE-2022-20815	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified CM Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) 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 the 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-2022-20800	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), and Cisco Unity Connection 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 the 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-2022-27168	Cross-site scripting vulnerability in LiteCart versions prior to 2.4.2 allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2022-35170	SAP NetWeaver Enterprise Portal does - versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, not sufficiently encode user-controlled inputs over the network, resulting in reflected Cross-Site Scripting (XSS) vulnerability, therefore changing the scope of the attack. This leads to limited impact on confidentiality and integrity of data.	6.1	More Details
CVE-2022-34007	EQS Integrity Line Professional through 2022-07-01 allows a stored XSS via a crafted whistleblower entry.	6.1	More Details
CVE-2022-1937	The Awin Data Feed WordPress plugin before 1.8 does not sanitise and escape a parameter before outputting it back via an AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-1910	The Shortcodes and extra features for Phlox WordPress plugin before 2.9.8 does not sanitise and escape a parameter before outputting it back in the response, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-32115	An issue in the isSVG() function of Known v1.2.2+2020061101 allows attackers to execute arbitrary code via a crafted SVG file.	6.1	More Details
CVE-2022-23713	A cross-site-scripting (XSS) vulnerability was discovered in the Vega Charts Kibana integration which could allow arbitrary JavaScript to be executed in a victim’s browser.	6.1	More Details
CVE-2022-22048	BitLocker Security Feature Bypass Vulnerability	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1474	The WP Event Manager WordPress plugin before 3.1.28 does not sanitise and escape its search before outputting it back in an attribute on the event dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-31904	EGT-Kommunikationstechnik UG Mediacenter before v2.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component Online_Update.php.	6.1	More Details
CVE-2022-32247	SAP NetWeaver Enterprise Portal - versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, is susceptible to script execution attack by an unauthenticated attacker due to improper sanitization of the User inputs while interacting on the Network. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	6.1	More Details
CVE-2022-33157	The libconnect extension before 7.0.8 and 8.x before 8.1.0 for TYPO3 allows XSS.	6.1	More Details
CVE-2022-33156	The matomo_integration (aka Matomo Integration) extension before 1.3.2 for TYPO3 allows XSS.	6.1	More Details
CVE-2022-35225	SAP NetWeaver Enterprise Portal - versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently encode user-controlled inputs over the network, resulting in reflected Cross-Site Scripting (XSS) vulnerability, therefore changing the scope of the attack. This leads to limited impact on confidentiality and integrity of data.	6.1	More Details
CVE-2021-31676	A reflected XSS was discovered in PESCMS-V2.3.3. When combined with CSRF in the same file, they can cause bigger destruction.	6.1	More Details
CVE-2022-35224	SAP Enterprise Portal - versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. This attack can be used to non-permanently deface or modify portal content. The execution of script content by a victim registered on the portal could compromise the confidentiality and integrity of victim&#65533;s web browser session.	6.1	More Details
CVE-2022-30517	Mogu blog 5.2 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2022-27910	In Joomla component 'Joomlatools - DOCman 3.5.13 (and likely most versions below)' are affected to an reflected Cross-Site Scripting (XSS) in an image upload function	6.1	More Details
CVE-2022-2353	Prior to microweber/microweber v1.2.20, due to improper neutralization of input, an attacker can steal tokens to perform cross-site request forgery, fetch contents from same-site and redirect a user.	6.1	More Details
CVE-2022-1220	The FoxyShop WordPress plugin before 4.8.2 does not sanitise and escape a parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-35416	H3C SSL VPN through 2022-07-10 allows wnm/login/login.json svpnlang cookie XSS.	6.1	More Details
CVE-2021-45721	JFrog Artifactory prior to version 7.29.8 and 6.23.38 is vulnerable to Reflected Cross-Site Scripting (XSS) through one of the XHR parameters in Users REST API endpoint. This issue affects: JFrog JFrog Artifactory JFrog Artifactory versions before 7.36.1 versions prior to 7.29.8; JFrog Artifactory versions before 6.23.41 versions prior to 6.23.38.	6.1	More Details
CVE-2022-35172	SAP NetWeaver Enterprise Portal - versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently encode user-controlled inputs, resulting in reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2022-35169	SAP BusinessObjects Business Intelligence Platform (LCM) - versions 420, 430, allows an attacker with an admin privilege to read and decrypt LCMBIAR file's password under certain conditions, enabling the attacker to modify the password or import the file into another system causing high impact on confidentiality but a limited impact on the availability and integrity of the application.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31133	HumHub is an Open Source Enterprise Social Network. Affected versions of HumHub are vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. For exploitation, the attacker would need a permission to administer the Spaces feature. The names of individual "spaces" are not properly escaped and so an attacker with sufficient privilege could insert malicious javascript into a space name and exploit system users who visit that space. It is recommended that the HumHub is upgraded to 1.11.4, 1.10.5. There are no known workarounds for this issue.	5.9	More Details
CVE-2022-25047	The password reset token in CWP v0.9.8.1126 is generated using known or predictable values.	5.9	More Details
CVE-2022-31139	UnsafeAccessor (UA) is a bridge to access jdk.internal.misc.Unsafe & sun.misc.Unsafe. Normally, if UA is loaded as a named module, the internal data of UA is protected by JVM and others can only access UA via UA's standard API. The main application can set up `SecurityCheck.AccessLimiter` for UA to limit access to UA. Starting with version 1.4.0 and prior to version 1.7.0, when `SecurityCheck.AccessLimiter` is set up, untrusted code can access UA without limitation, even when UA is loaded as a named module. This issue does not affect those for whom `SecurityCheck.AccessLimiter` is not set up. Version 1.7.0 contains a patch.	5.9	More Details
CVE-2022-32208	When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw makes it possible for a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client.	5.9	More Details
CVE-2022-31029	AdminLTE is a Pi-hole Dashboard for stats and configuration. In affected versions inserting code like `<script>alert("XSS")</script>` in the field marked with "Domain to look for" and hitting <kbd>enter</kbd> (or clicking on any of the buttons) will execute the script. The user must be logged in to use this vulnerability. Usually only administrators have login access to pi-hole, minimizing the risks. Users are advised to upgrade. There are no known workarounds for this issue.	5.9	More Details
CVE-2022-22028	Windows Network File System Information Disclosure Vulnerability	5.9	More Details
CVE-2022-30619	Editable SQL Queries behind Base64 encoding sending from the Client-Side to The Server-Side for a particular API used in legacy Work Center module. He attack is available for any authenticated user, in any kind of rule. under the function : /AgilePointServer/Extension/FetchUsingEncodedData in the parameter: EncodedData	5.9	More Details
CVE-2022-22711	Windows BitLocker Information Disclosure Vulnerability	5.7	More Details
CVE-2022-30223	Windows Hyper-V Information Disclosure Vulnerability	5.7	More Details
CVE-2022-29901	Intel microprocessor generations 6 to 8 are affected by a new Spectre variant that is able to bypass their retpoline mitigation in the kernel to leak arbitrary data. An attacker with unprivileged user access can hijack return instructions to achieve arbitrary speculative code execution under certain microarchitecture-dependent conditions.	5.6	More Details
CVE-2022-2366	Incorrect default configuration for trusted IP header in Mattermost version 6.7.0 and earlier allows attacker to bypass some of the rate limitations in place or use manipulated IPs for audit logging via manipulating the request headers.	5.6	More Details
CVE-2022-34464	A vulnerability has been identified in SICAM GridEdge Essential ARM (All versions), SICAM GridEdge Essential Intel (All versions < V2.7.3), SICAM GridEdge Essential with GDS ARM (All versions), SICAM GridEdge Essential with GDS Intel (All versions < V2.7.3). Affected software uses an improperly protected file to import SSH keys. Attackers with access to the filesystem of the host on which SICAM GridEdge runs, are able to inject a custom SSH key to that file.	5.5	More Details
CVE-2022-23173	this vulnerability affect user that even not allowed to access via the web interface. First of all, the attacker needs to access the "Login menu - demo site" then he can see in this menu all the functionality of the application. If the attacker will try to click on one of the links, he will get an answer that he is not authorized because he needs to log in with credentials. after he performed log in to the system there are some functionalities that the specific user is not allowed to perform because he was configured with low privileges however all the attacker need to do in order to achieve his goals is to change the value of the prog step parameter from 0 to 1 or more and then the attacker could access to some of the functionality the web application that he couldn't perform it before the parameter changed.	5.5	More Details
CVE-2022-30213	Windows GDI+ Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1794	The CODESYS OPC DA Server prior V3.5.18.20 stores PLC passwords as plain text in its configuration file so that it is visible to all authorized Microsoft Windows users of the system.	5.5	More Details
CVE-2022-34282	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-047)	5.5	More Details
CVE-2020-4138	IBM SiteProtector Appliance 3.1.1 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 174049.	5.5	More Details
CVE-2022-35171	When a user opens manipulated JPEG 2000 (.jp2, jp2k.x3d) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application. The file format details along with their CVE relevant information can be found below	5.5	More Details
CVE-2022-23172	An attacker can access to "Forgot my password" button, as soon as he puts users is valid in the system, the system would issue a message that a password reset email had been sent to user. This way you can verify which users are in the system and which are not.	5.5	More Details
CVE-2022-34285	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-050)	5.5	More Details
CVE-2022-33711	Improper validation of integrity check vulnerability in Samsung USB Driver Windows Installer for Mobile Phones prior to version 1.7.56.0 allows local attackers to delete arbitrary directory using directory junction.	5.5	More Details
CVE-2022-34283	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-048)	5.5	More Details
CVE-2011-4916	Linux kernel through 3.1 allows local users to obtain sensitive keystroke information via access to /dev/pts/ and /dev/tty*.	5.5	More Details
CVE-2022-2318	There are use-after-free vulnerabilities caused by timer handler in net/rose/rose_timer.c of linux that allow attackers to crash linux kernel without any privileges.	5.5	More Details
CVE-2022-34291	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains a stack corruption vulnerability while parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-057, FG-VD-22-058, FG-VD-22-060)	5.5	More Details
CVE-2022-34287	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains a stack corruption vulnerability while parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-052, FG-VD-22-056)	5.5	More Details
CVE-2022-34290	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains a stack corruption vulnerability while parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-055)	5.5	More Details
CVE-2022-34288	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-053)	5.5	More Details
CVE-2022-21763	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708.	5.5	More Details
CVE-2022-32441	A memory corruption in Hex Rays Ida Pro v6.6 allows attackers to cause a Denial of Service (DoS) via a crafted file. Related to Data from Faulting Address controls subsequent Write Address starting at msvcrt!memcpy+0x0000000000000056.	5.5	More Details
CVE-2022-21764	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33155	The ameos_tarteaucitron (aka AMEOS - TarteAuCitron GDPR cookie banner and tracking management / French RGPD compatible) extension before 1.2.23 for TYPO3 allows XSS.	5.4	More Details
CVE-2022-34167	IBM CICS TX Standard and Advanced 11.1 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: 229432.	5.4	More Details
CVE-2022-34166	IBM CICS TX Standard and Advanced 11.1 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: 229430.	5.4	More Details
CVE-2022-2316	HTML injection vulnerability in secure messages of Devolutions Server before 2022.2 allows attackers to alter the rendering of the page or redirect a user to another site.	5.4	More Details
CVE-2022-33154	The schema (aka Embedding schema.org vocabulary) extension before 1.13.1 and 2.x before 2.5.1 for TYPO3 allows XSS.	5.4	More Details
CVE-2022-2342	Cross-site Scripting (XSS) - Stored in GitHub repository outline/outline prior to v0.64.4.	5.4	More Details
CVE-2015-3172	EidoGo is susceptible to Cross-Site Scripting (XSS) attacks via maliciously crafted SGF input.	5.4	More Details
CVE-2022-1938	The Awin Data Feed WordPress plugin before 1.8 does not sanitise and escape a header when processing request to generate analytics data, allowing unauthenticated users to perform Stored Cross-Site Scripting attacks against a logged in admin viewing the plugin's settings	5.4	More Details
CVE-2022-31131	Nextcloud mail is a Mail app for the Nextcloud home server product. Versions of Nextcloud mail prior to 1.12.2 were found to be missing user account ownership checks when performing tasks related to mail attachments. Attachments may have been exposed to incorrect system users. It is recommended that the Nextcloud Mail app is upgraded to 1.12.2. There are no known workarounds for this issue. ### Workarounds No workaround available ### References * [Pull request] (https://github.com/nextcloud/mail/pull/6600) * [HackerOne](https://hackerone.com/reports/1579820) ### For more information If you have any questions or comments about this advisory: * Create a post in [nextcloud/security-advisories] (https://github.com/nextcloud/security-advisories/discussions) * Customers: Open a support ticket at [support.nextcloud.com] (https://support.nextcloud.com)	5.4	More Details
CVE-2022-34306	IBM CICS TX Standard and Advanced 11.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 229435.	5.4	More Details
CVE-2022-25875	The package svelte before 3.49.0 are vulnerable to Cross-site Scripting (XSS) due to improper input sanitization and to improper escape of attributes when using objects during SSR (Server-Side Rendering). Exploiting this vulnerability is possible via objects with a custom toString() function.	5.4	More Details
CVE-2022-34160	IBM CICS TX Standard and Advanced 11.1 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 229330.	5.4	More Details
CVE-2022-1626	The Sharebar WordPress plugin through 1.4.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and also lead to Stored Cross-Site Scripting issue due to the lack of sanitisation and escaping in some of them	5.4	More Details
CVE-2022-31597	Within SAP S/4HANA - versions S4CORE 101, 102, 103, 104, 105, 106, SAPSCORE 127, the application business partner extension for Spain/Slovakia does not perform necessary authorization checks for a low privileged authenticated user over the network, resulting in escalation of privileges leading to low impact on confidentiality and integrity of the data.	5.4	More Details
CVE-2022-1757	The pagebar WordPress plugin before 2.70 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack. Furthermore, due to the lack of sanitisation in some of them, it could also lead to Stored XSS issues	5.4	More Details
CVE-2022-31598	Due to insufficient input validation, SAP Business Objects - version 420, allows an authenticated attacker to submit a malicious request through an allowed operation. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22370	IBM Security Verify Access 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 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: 221194.	5.4	More Details
CVE-2022-31290	A cross-site scripting (XSS) vulnerability in Known v1.2.2+2020061101 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Your Name text field.	5.4	More Details
CVE-2022-31654	VMware vRealize Log Insight in versions prior to 8.8.2 contain a stored cross-site scripting vulnerability due to improper input sanitization in configurations.	5.4	More Details
CVE-2022-25303	The package whoogle-search before 0.7.2 are vulnerable to Cross-site Scripting (XSS) via the query string parameter q. In the case where it does not contain the http string, it is used to build the error_message that is then rendered in the error.html template, using the [flask.render_template](https://flask.palletsprojects.com/en/2.1.x/api/flask.render_template) function. However, the error_message is rendered using the [| safe filter](https://jinja.palletsprojects.com/en/3.1.x/templates/working-with-automatic-escaping), meaning the user input is not escaped.	5.4	More Details
CVE-2022-31655	VMware vRealize Log Insight in versions prior to 8.8.2 contain a stored cross-site scripting vulnerability due to improper input sanitization in alerts.	5.4	More Details
CVE-2022-2365	Cross-site Scripting (XSS) - Stored in GitHub repository zadam/trilium prior to 0.53.3.	5.4	More Details
CVE-2022-29602	The gridelements (aka Grid Elements) extension through 7.6.1, 8.x through 8.7.0, 9.x through 9.7.0, and 10.x through 10.2.0 extension for TYPO3 allows XSS.	5.4	More Details
CVE-2022-24141	The iTopVPNmini.exe component of iTop VPN 3.2 will try to connect to datastate_iTopVPN_Pipe_Server on a loop. An attacker that opened a named pipe with the same name can use it to gain the token of another user by listening for connections and abusing ImpersonateNamedPipeClient().	5.4	More Details
CVE-2022-32567	The Appfire Jira Misc Custom Fields (JMCF) app 2.4.6 for Atlassian Jira allows XSS via a crafted project name to the Add Auto Indexing Rule function.	5.4	More Details
CVE-2022-33712	Intent redirection vulnerability using implict intent in Camera prior to versions 12.0.01.64 ,12.0.3.23, 12.0.0.98, 12.0.6.11, 12.0.3.19 in Android S(12) allows attacker to get sensitive information.	5.3	More Details
CVE-2022-33911	An issue was discovered in Couchbase Server 7.x before 7.0.4. Field names are not redacted in logged validation messages for Analytics Service. An Unauthorized Actor may be able to obtain Sensitive Information.	5.3	More Details
CVE-2015-3207	In Openshift Origin 3 the cookies being set in console have no 'secure', 'HttpOnly' attributes.	5.3	More Details
CVE-2022-20752	A vulnerability in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to perform a timing attack. This vulnerability is due to insufficient protection of a system password. An attacker could exploit this vulnerability by observing the time it takes the system to respond to various queries. A successful exploit could allow the attacker to determine a sensitive system password.	5.3	More Details
CVE-2022-33707	Improper identifier creation logic in Find My Mobile prior to version 7.2.24.12 allows attacker to identify the device.	5.3	More Details
CVE-2020-29508	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.6, contain an Improper Input Validation Vulnerability.	5.3	More Details
CVE-2020-29507	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.4, and Dell BSAFE Micro Edition Suite, versions before 4.4, contain an Improper Input Validation Vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31111	Frontier is Substrate's Ethereum compatibility layer. In affected versions the truncation done when converting between EVM balance type and Substrate balance type was incorrectly implemented. This leads to possible discrepancy between appeared EVM transfer value and actual Substrate value transferred. It is recommended that an emergency upgrade to be planned and EVM execution temporarily paused in the mean time. The issue is patched in Frontier master branch commit fed5e0a9577c10bea021721e8c2c5c378e16bf66 and polkadot-v0.9.22 branch commit e3e427fa2e5d1200a784679f8015d4774cedc934. This vulnerability affects only EVM internal states, but not Substrate balance states or node. You can temporarily pause EVM execution (by setting up a Substrate `CallFilter` that disables `pallet-evm` and `pallet-ethereum` calls before the patch can be applied.	5.3	More Details
CVE-2020-35163	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.6, contain a Use of Insufficiently Random Values Vulnerability.	5.3	More Details
CVE-2021-39041	IBM QRadar SIEM 7.3, 7.4, and 7.5 may be vulnerable to partial denial of service attack, resulting in some protocols not listening to specified ports. IBM X-Force ID: 214028.	5.3	More Details
CVE-2021-41042	In Eclipse Lyo versions 1.0.0 to 4.1.0, a TransformerFactory is initialized with the defaults that do not restrict DTD loading when working with RDF/XML. This allows an attacker to cause an external DTD to be retrieved.	5.3	More Details
CVE-2022-32248	Due to missing input validation in the Manage Checkbooks component of SAP S/4HANA - version 101, 102, 103, 104, 105, 106, an attacker could insert or edit the value of an existing field in the database. This leads to an impact on the integrity of the data.	5.3	More Details
CVE-2020-35166	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.6, contain an Observable Timing Discrepancy Vulnerability.	5.1	More Details
CVE-2022-33695	Use of improper permission in InputManagerService prior to SMR Jul-2022 Release 1 allows unauthorized access to the service.	5.1	More Details
CVE-2022-35412	Digital Guardian Agent 7.7.4.0042 allows an administrator (who ordinarily does not have a supported way to uninstall the product) to disable some of the agent functionality and then exfiltrate files to an external USB device.	5.1	More Details
CVE-2021-46687	JFrog Artifactory prior to version 7.31.10 and 6.23.38 is vulnerable to Sensitive Data Exposure through the Project Administrator REST API. This issue affects: JFrog JFrog Artifactory JFrog Artifactory versions before 7.31.10 versions prior to 7.x; JFrog Artifactory versions before 6.23.38 versions prior to 6.x.	4.9	More Details
CVE-2022-33671	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-31134	Zulip is an open-source team collaboration tool. Zulip Server versions 2.1.0 above have a user interface tool, accessible only to server owners and server administrators, which provides a way to download a "public data" export. While this export is only accessible to administrators, in many configurations server administrators are not expected to have access to private messages and private streams. However, the "public data" export which administrators could generate contained the attachment contents for all attachments, even those from private messages and streams. Zulip Server version 5.4 contains a patch for this issue.	4.9	More Details
CVE-2022-33669	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-33650	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-33668	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-33658	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20768	A vulnerability in the logging component of Cisco TelePresence Collaboration Endpoint (CE) and RoomOS Software could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. This vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs on an affected system and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to access confidential information, some of which may contain personally identifiable information (PII). Note: To access the logs that are stored in the RoomOS Cloud, an attacker would need valid Administrator-level credentials.	4.9	More Details
CVE-2022-33642	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-33652	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-33653	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-33654	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-33651	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-33659	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-33660	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-33664	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-27548	HCL Launch stores user credentials in plain clear text which can be read by a local user.	4.9	More Details
CVE-2022-31075	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, EdgeCore may be susceptible to a DoS attack on CloudHub if an attacker was to send a well-crafted HTTP request to `/edge.crt`. If an attacker can send a well-crafted HTTP request to CloudHub, and that request has a very large body, that request can crash the HTTP service through a memory exhaustion vector. The request body is being read into memory, and a body that is larger than the available memory can lead to a successful attack. Because the request would have to make it through authorization, only authorized users may perform this attack. The consequence of the exhaustion is that CloudHub will be in denial of service. KubeEdge is affected only when users enable the CloudHub module in the file `cloudcore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the CloudHub switch in the config file `cloudcore.yaml`.	4.9	More Details
CVE-2022-1894	The Popup Builder WordPress plugin before 4.1.11 does not escape and sanitize some settings, which could allow high privilege users to perform Stored Cross-Site Scripting attacks when the unfiltred_html is disallowed	4.8	More Details
CVE-2022-28624	A potential security vulnerability has been identified in certain HPE FlexNetwork and FlexFabric switch products. The vulnerability could be remotely exploited to allow cross site scripting (XSS). HPE has made the following software updates to resolve the vulnerability. HPE FlexNetwork 5130EL_7.10.R3507P02 and HPE FlexFabric 5945_7.10.R6635.	4.8	More Details
CVE-2022-2050	The WP-Paginate WordPress plugin before 2.1.9 does not escape one of its settings, which could allow high privilege users to perform Stored Cross-Site Scripting attacks when unfiltered_html is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32061	An arbitrary file upload vulnerability in the Select User function under the People Menu component of Snipe-IT v6.0.2 allows attackers to execute arbitrary code via a crafted file.	4.8	More Details
CVE-2022-32060	An arbitrary file upload vulnerability in the Update Branding Settings component of Snipe-IT v6.0.2 allows attackers to execute arbitrary code via a crafted file.	4.8	More Details
CVE-2022-2089	The Bold Page Builder WordPress plugin before 4.3.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	4.8	More Details
CVE-2022-2093	The WP Duplicate Page WordPress plugin before 1.3 does not sanitize and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	4.8	More Details
CVE-2020-35167	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.6, contain an Observable Timing Discrepancy Vulnerability.	4.8	More Details
CVE-2022-2263	A vulnerability was found in Online Hotel Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file edit_room_cat.php of the component Room Handler. The manipulation of the argument roomname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2022-33632	Microsoft Office Security Feature Bypass Vulnerability	4.7	More Details
CVE-2020-35168	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.6, contain an Observable Timing Discrepancy Vulnerability.	4.7	More Details
CVE-2022-30212	Windows Connected Devices Platform Service Information Disclosure Vulnerability	4.7	More Details
CVE-2022-30187	Azure Storage Library Information Disclosure Vulnerability	4.7	More Details
CVE-2022-21845	Windows Kernel Information Disclosure Vulnerability	4.7	More Details
CVE-2022-2262	A vulnerability has been found in Online Hotel Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file edit_all_room.php of the component Room Handler. The manipulation of the argument id with the input 2828%27%20AND%20(SELECT%203766%20FROM%20(SELECT(SLEEP(5)))BmIK)%20AND%20%27YLPl%27=%27YLPl leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2022-32246	SAP Busines Objects Business Intelligence Platform (Visual Difference Application) - versions 420, 430, allows an authenticated attacker who has access to BI admin console to send crafted queries and extract data from the SQL backend. On successful exploitation, the attacker can cause limited impact on confidentiality and integrity of the application	4.6	More Details
CVE-2021-3696	A heap out-of-bounds write may heppen during the handling of Huffman tables in the PNG reader. This may lead to data corruption in the heap space. Confidentiality, Integrity and Availablity impact may be considered Low as it's very complex to an attacker control the encoding and positioning of corrupted Huffman entries to achieve results such as arbitrary code execution and/or secure boot circumvention. This flaw affects grub2 versions prior grub-2.12.	4.5	More Details
CVE-2022-31074	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, several endpoints in the Cloud AdmissionController may be susceptible to a DoS attack if an HTTP request containing a very large Body is sent to it. The consequence of the exhaustion is that the Cloud AdmissionController will be in denial of service. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. There is currently no known workaround.	4.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3695	A crafted 16-bit grayscale PNG image may lead to a out-of-bounds write in the heap area. An attacker may take advantage of that to cause heap data corruption or eventually arbitrary code execution and circumvent secure boot protections. This issue has a high complexity to be exploited as an attacker needs to perform some triage over the heap layout to achieve signifcant results, also the values written into the memory are repeated three times in a row making difficult to produce valid payloads. This flaw affects grub2 versions prior grub-2.12.	4.5	More Details
CVE-2022-31080	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, a large response received by the viaduct WSClient can cause a DoS from memory exhaustion. The entire body of the response is being read into memory which could allow an attacker to send a request that returns a response with a large body. The consequence of the exhaustion is that the process which invokes a WSClient will be in a denial of service. The software is affected If users who are authenticated to the edge side connect to `cloudhub` from the edge side through WebSocket protocol. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. There are currently no known workarounds.	4.4	More Details
CVE-2022-31079	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the Cloud Stream server and the Edge Stream server reads the entire message into memory without imposing a limit on the size of this message. An attacker can exploit this by sending a large message to exhaust memory and cause a DoS. The Cloud Stream server and the Edge Stream server are under DoS attack in this case. The consequence of the exhaustion is that the CloudCore and EdgeCore will be in a denial of service. Only an authenticated user can cause this issue. It will be affected only when users enable `cloudStream` module in the config file `cloudcore.yaml` and enable `edgeStream` module in the config file `edgecore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable cloudStream module in the config file `cloudcore.yaml` and disable edgeStream module in the config file `edgecore.yaml`.	4.4	More Details
CVE-2022-31078	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the CloudCore Router does not impose a limit on the size of responses to requests made by the REST handler. An attacker could use this weakness to make a request that will return an HTTP response with a large body and cause DoS of CloudCore. In the HTTP Handler API, the rest handler makes a request to a pre-specified handle. The handle will return an HTTP response that is then read into memory. The consequence of the exhaustion is that CloudCore will be in a denial of service. Only an authenticated user of the cloud can make an attack. It will be affected only when users enable `router` module in the config file `cloudcore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the router switch in the config file `cloudcore.yaml`.	4.4	More Details
CVE-2022-21769	In CCCI, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641687.	4.4	More Details
CVE-2021-37839	Apache Superset up to 1.5.1 allowed for authenticated users to access metadata information related to datasets they have no permission on. This metadata included the dataset name, columns and metrics.	4.3	More Details
CVE-2022-32290	The client in Northern.tech Mender 3.2.0, 3.2.1, and 3.2.2 has Incorrect Access Control. It listens on a random, unprivileged TCP port and exposes an HTTP proxy to facilitate API calls from additional client components running on the device. However, it listens on all network interfaces instead of only the localhost interface. Therefore, any client on the same network can connect to this TCP port and send HTTP requests. The Mender Client will forward these requests to the Mender Server. Additionally, if mTLS is set up, the Mender Client will connect to the Mender Server using the device's client certificate, making it possible for the attacker to bypass mTLS authentication and send requests to the Mender Server without direct access to the client certificate and related private key. Accessing the HTTP proxy from the local network doesn't represent a direct threat, because it doesn't expose any device or server-specific data. However, it increases the attack surface and can be a potential vector to exploit other vulnerabilities both on the Client and the Server.	4.3	More Details
CVE-2022-31592	The application SAP Enterprise Extension Defense Forces & Public Security - versions 605, 606, 616,617,618, 802, 803, 804, 805, 806, does not perform necessary authorization checks for an authenticated user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality.	4.3	More Details
CVE-2022-2291	A vulnerability was found in SourceCodester Hotel Management System 2.0. It has been rated as problematic. This issue affects some unknown processing of the file /ci_hms/search of the component Search. The manipulation of the argument search with the input "><script>alert("XSS")</script> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2022-35406	A URL disclosure issue was discovered in Burp Suite before 2022.6. If a user views a crafted response in the Repeater or Intruder, it may be incorrectly interpreted as a redirect.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20862	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to read arbitrary files on the underlying operating system of an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to access sensitive files on the operating system.	4.3	More Details
CVE-2022-30852	Known v1.3.1 was discovered to contain an Insecure Direct Object Reference (IDOR).	4.3	More Details
CVE-2022-2123	The WP Opt-in WordPress plugin through 1.4.1 is vulnerable to CSRF which allows changed plugin settings and can be used for sending spam emails.	4.3	More Details
CVE-2022-1957	The Comment License WordPress plugin before 1.4.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2022-1956	The Shortcut Macros WordPress plugin through 1.3 does not have authorisation and CSRF checks in place when updating its settings, which could allow any authenticated users, such as subscriber, to update them.	4.3	More Details
CVE-2022-32205	A malicious server can serve excessive amounts of `Set-Cookie:` headers in a HTTP response to curl and curl < 7.84.0 stores all of them. A sufficiently large amount of (big) cookies make subsequent HTTP requests to this, or other servers to which the cookies match, create requests that become larger than the threshold that curl uses internally to avoid sending crazy large requests (1048576 bytes) and instead returns an error.This denial state might remain for as long as the same cookies are kept, match and haven't expired. Due to cookie matching rules, a server on `foo.example.com` can set cookies that also would match for `bar.example.com`, making it it possible for a "sister server" to effectively cause a denial of service for a sibling site on the same second level domain using this method.	4.3	More Details
CVE-2022-31472	Browse restriction bypass vulnerability in Cabinet of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to obtain the data of Cabinet.	4.3	More Details
CVE-2022-30943	Browsing restriction bypass vulnerability in Bulletin of Cybozu Garoon 4.0.0 to 5.9.1 allows a remote authenticated attacker to obtain the data of Bulletin.	4.3	More Details
CVE-2022-28889	In Apache Druid 0.22.1 and earlier, the server did not set appropriate headers to prevent clickjacking. Druid 0.23.0 and later prevent clickjacking using the Content-Security-Policy header.	4.3	More Details
CVE-2022-27549	HCL Launch may store certain data for recurring activities in a plain text format.	4.0	More Details
CVE-2022-33692	Exposure of Sensitive Information in Messaging application prior to SMR Jul-2022 Release 1 allows local attacker to access imsi and iccid via log.	4.0	More Details
CVE-2022-30757	Improper authorization in isemtelephony prior to SMR Jul-2022 Release 1 allows attacker to obtain CID without ACCESS_FINE_LOCATION permission.	4.0	More Details
CVE-2022-30758	Implicit Intent hijacking vulnerability in Finder prior to SMR Jul-2022 Release 1 allow allows attackers to access some protected information with privilege of Finder.	4.0	More Details
CVE-2022-33685	Unprotected dynamic receiver in Wearable Manager Service prior to SMR Jul-2022 Release 1 allows attacker to launch arbitray activity and access senstive information.	4.0	More Details
CVE-2022-33690	Improper input validation in Contacts Storage prior to SMR Jul-2022 Release 1 allows attacker to access arbitrary file.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33694	Exposure of Sensitive Information in CSC application prior to SMR Jul-2022 Release 1 allows local attacker to access wifi information via unprotected intent broadcasting.	4.0	More Details
CVE-2022-33696	Exposure of Sensitive Information in Telephony service prior to SMR Jul-2022 Release 1 allows local attacker to access imsi and iccid via log.	4.0	More Details
CVE-2022-35229	An authenticated user can create a link with reflected Javascript code inside it for the discovery page and send it to other users. The payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict.	3.7	More Details
CVE-2022-35230	An authenticated user can create a link with reflected Javascript code inside it for the graphs page and send it to other users. The payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict.	3.7	More Details
CVE-2022-2363	A vulnerability, which was classified as problematic, has been found in SourceCodester Simple Parking Management System 1.0. Affected by this issue is some unknown functionality of the file /ci_spms/admin/search/searching/. The manipulation of the argument search with the input "><script>alert("XSS")</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-2364	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Parking Management System 1.0. This affects an unknown part of the file /ci_spms/admin/category. The manipulation of the argument vehicle_type with the input "><script>alert("XSS")</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-2293	A vulnerability classified as problematic was found in SourceCodester Simple Sales Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /ci_ssms/index.php/orders/create. The manipulation of the argument customer_name with the input <script>alert("XSS")</script> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-2292	A vulnerability classified as problematic has been found in SourceCodester Hotel Management System 2.0. Affected is an unknown function of the file /ci_hms/massage_room/edit/1 of the component Room Edit Page. The manipulation of the argument massageroomDetails with the input "><script>alert("XSS")</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-33705	Information exposure in Calendar prior to version 12.3.05.10000 allows attacker to access calendar schedule without READ_CALENDAR permission.	3.3	More Details
CVE-2022-30751	Improper access control vulnerability in sendDHCPACKBroadcast function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected by using WIFI_AP_STA_DHCPACK_EVENT action.	3.3	More Details
CVE-2022-33701	Improper access control vulnerability in KnoxCustomManagerService prior to SMR Jul-2022 Release 1 allows attacker to call PowerManaer.goToSleep method which is protected by system permission by sending braodcast intent.	3.3	More Details
CVE-2022-30750	Improper access control vulnerability in updateLastConnectedClientInfo function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected.	3.3	More Details
CVE-2022-30752	Improper access control vulnerability in sendDHCPACKBroadcast function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected by using WIFI_AP_STA_STATE_CHANGED action.	3.3	More Details
CVE-2022-33687	Exposure of Sensitive Information in telephony-common.jar prior to SMR Jul-2022 Release 1 allows local attackers to access IMSI via log.	3.3	More Details
CVE-2022-30753	Improper use of a unique device ID in unprotected SecSoterService prior to SMR Jul-2022 Release 1 allows local attackers to get the device ID without permission.	3.3	More Details
CVE-2022-33698	Exposure of Sensitive Information in Telecom application prior to SMR Jul-2022 Release 1 allows local attackers to access ICCID via log.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33697	Sensitive information exposure vulnerability in ImsServiceSwitchBase in ImsCore prior to SMR Jul-2022 Release 1 allows local attackers with log access permission to get IMSI through device log.	3.3	More Details
CVE-2022-33688	Sensitive information exposure vulnerability in EventType in SecTelephonyProvider prior to SMR Jul-2022 Release 1 allows local attackers with log access permission to get IMSI through device log.	3.3	More Details
CVE-2021-23163	JFrog Artifactory prior to version 7.33.6 and 6.23.38, is vulnerable to CSRF (Cross-Site Request Forgery) for specific endpoints. This issue affects: JFrog JFrog Artifactory JFrog Artifactory versions before 7.33.6 versions prior to 7.x; JFrog Artifactory versions before 6.23.38 versions prior to 6.x.	3.1	More Details
CVE-2022-2047	In Eclipse Jetty versions 9.4.0 thru 9.4.46, and 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, the parsing of the authority segment of an http scheme URI, the Jetty HttpURI class improperly detects an invalid input as a hostname. This can lead to failures in a Proxy scenario.	2.7	More Details
CVE-2022-35648	Nautilus treadmills T616 S/N 100672PRO21140001 through 100672PRO21171980 and T618 S/N 100647PRO21130111 through 100647PRO21183960 with software before 2022-06-09 allow physically proximate attackers to cause a denial of service (fall) by connecting the power cord to a 120V circuit (which may lead to self-starting at an inopportune time).	2.6	More Details
CVE-2022-31102	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Argo CD starting with 2.3.0 and prior to 2.3.6 and 2.4.5 is vulnerable to a cross-site scripting (XSS) bug which could allow an attacker to inject arbitrary JavaScript in the `/auth/callback` page in a victim's browser. This vulnerability only affects Argo CD instances which have single sign on (SSO) enabled. The exploit also assumes the attacker has 1) access to the API server's encryption key, 2) a method to add a cookie to the victim's browser, and 3) the ability to convince the victim to visit a malicious `/auth/callback` link. The vulnerability is classified as low severity because access to the API server's encryption key already grants a high level of access. Exploiting the XSS would allow the attacker to impersonate the victim, but would not grant any privileges which the attacker could not otherwise gain using the encryption key. A patch for this vulnerability has been released in the following Argo CD versions 2.4.5 and 2.3.6. There is currently no known workaround.	2.6	More Details
CVE-2022-33706	Improper access control vulnerability in Samsung Gallery prior to version 13.1.05.8 allows physical attackers to access the pictures using S Pen air gesture.	2.4	More Details
CVE-2022-23744	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator.	2.3	More Details
CVE-2022-33686	Exposure of Sensitive Information in GsmAlarmManager prior to SMR Jul-2022 Release 1 allows local attacker to access iccid via log.	2.3	More Details
CVE-2022-33693	Exposure of Sensitive Information in CID Manager prior to SMR Jul-2022 Release 1 allows local attacker to access iccid via log.	2.0	More Details
CVE-2022-33699	Exposure of Sensitive Information in getDsaSimImsi in TelephonyUI prior to SMR Jul-2022 Release 1 allows local attacker to access imsi via log.	2.0	More Details
CVE-2022-33700	Exposure of Sensitive Information in putDsaSimImsi in TelephonyUI prior to SMR Jul-2022 Release 1 allows local attacker to access imsi via log.	2.0	More Details
CVE-2014-8113	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-2014-2887	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-2014-2895	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-2022-32951	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-1926	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-2014-3588	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-2014-0024	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-2014-3644	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-2014-3658	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-2014-3705	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-2014-3918	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-2014-7854	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-2014-3516	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-2022-35339	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2019-19152	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2015-5596	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-4332	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-4169	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-4102	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-4101	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-3377	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-3266	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-3265	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-3264	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-3263	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-3262	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-3261	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-3260	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-2671	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-2236	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-1871	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-1837	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-0281	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-0280	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-0256	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-5328	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-5597	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2019-19153	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-5598	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2019-19154	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2022-35300	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2019-19156	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-19157	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-19158	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-19159	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2020-25585	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-25586	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-25587	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-25588	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-25589	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-25590	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-25591	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2022-29926	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation in Cybozu, Inc. showed that it was not a vulnerability. Notes: https://jvn.jp/en/jp/JVN14077132	N/A	More Details
CVE-2020-27731	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-27732	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31569	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that no specific affected product had been identified. Notes: none	N/A	More Details
CVE-2015-8819	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2015-7800	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2015. Notes: none	N/A	More Details
CVE-2019-19155	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2022-35303	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35301	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35387	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35365	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35366	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35367	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35368	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35369	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35370	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35371	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35372	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35373	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35374	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35375	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35376	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35377	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35378	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35379	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35380	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35381	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35382	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35383	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35384	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35385	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35364	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35363	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35362	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35350	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35341	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35342	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35343	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35344	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35345	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35346	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35347	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35348	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35349	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35351	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35361	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35352	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35353	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35354	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35355	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35356	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35357	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35358	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35359	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35360	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35386	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35388	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35302	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35389	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35324	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35323	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35322	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35321	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35319	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35318	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35317	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35316	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35315	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35314	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35313	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35312	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35311	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35310	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35309	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35308	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35307	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35306	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35305	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35304	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35340	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35325	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35326	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35327	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35399	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35390	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35391	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35392	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35393	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35394	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35395	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35396	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35397	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35398	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35338	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35328	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35337	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35336	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35335	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35334	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35333	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35332	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35331	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35330	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35329	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35320	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details