SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 August 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-2022-32292	In ConnMan through 1.41, remote attackers able to send HTTP requests to the gweb component are able to exploit a heap-based buffer overflow in received_data to execute code.	9.8	More Details
CVE-2022-24024	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the rtk_ate binary.	9.8	More Details
CVE-2022-25996	A stack-based buffer overflow vulnerability exists in the confsrv addTimeGroup functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to a buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.	9.8	More Details
CVE-2022-24029	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the rp-pppoe.so binary.	9.8	More Details
CVE-2022-24028	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the libcommonprod.so binary.	9.8	More Details
CVE-2022-24027	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the libcommon.so binary.	9.8	More Details
CVE-2022-24026	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the telnet_ate_monitor binary.	9.8	More Details
CVE-2022-24025	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the sntp binary.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24022	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the pannn binary.	9.8	More Details
CVE-2022-34974	D-Link DIR810LA1_FW102B22 was discovered to contain a command injection vulnerability via the Ping_addr function.	9.8	More Details
CVE-2022-24021	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the online_process binary.	9.8	More Details
CVE-2022-24020	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the network_check binary.	9.8	More Details
CVE-2022-24019	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the netctrl binary.	9.8	More Details
CVE-2022-24018	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the multiWAN binary.	9.8	More Details
CVE-2022-24017	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the miniupnpd binary.	9.8	More Details
CVE-2022-24016	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the mesh_status_check binary.	9.8	More Details
CVE-2022-26009	A stack-based buffer overflow vulnerability exists in the confsrv ucloud_set_node_location functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.	9.8	More Details
CVE-2022-26342	A buffer overflow vulnerability exists in the confsrv ucloud_set_node_location functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to a buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.	9.8	More Details
CVE-2022-26346	A denial of service vulnerability exists in the ucloud_del_node functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to trigger this vulnerability.	9.8	More Details
CVE-2022-26376	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.	9.8	More Details
CVE-2022-27178	A denial of service vulnerability exists in the confctl_set_wan_cfg functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to trigger this vulnerability.	9.8	More Details
CVE-2022-27631	A memory corruption vulnerability exists in the httpd unescape functionality of DD-WRT Revision 32270 - Revision 48599. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28664	A memory corruption vulnerability exists in the httpd unescape functionality of FreshTomato 2022.1. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.The `freshtomato-mips` has a vulnerable URL-decoding feature that can lead to memory corruption.	9.8	More Details
CVE-2022-28665	A memory corruption vulnerability exists in the httpd unescape functionality of FreshTomato 2022.1. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.The `freshtomato-arm` has a vulnerable URL-decoding feature that can lead to memory corruption.	9.8	More Details
CVE-2022-29465	An out-of-bounds write vulnerability exists in the PSD Header processing memory allocation functionality of Accusoft ImageGear 20.0. A specially-crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2022-37452	Exim before 4.95 has a heap-based buffer overflow for the alias list in host_name_lookup in host.c when sender_host_name is set.	9.8	More Details
CVE-2022-2269	The Website File Changes Monitor WordPress plugin before 1.8.3 does not sanitise and escape user input before using it in a SQL statement via an action available to users with the manage_options capability (by default admins), leading to an SQL injection	9.8	More Details
CVE-2022-2460	The WPDating WordPress plugin before 7.4.0 does not properly escape user input before concatenating it to certain SQL queries, leading to multiple SQL injection vulnerabilities exploitable by unauthenticated users	9.8	More Details
CVE-2022-35490	Zammad 5.2.0 is vulnerable to privilege escalation. Zammad has a prevention against brute-force attacks trying to guess login credentials. After a configurable amount of attempts, users are invalidated and logins prevented. An attacker might work around this prevention, enabling them to send more than the configured amount of requests before the user invalidation takes place.	9.8	More Details
CVE-2022-2713	Insufficient Session Expiration in GitHub repository cockpit-hq/cockpit prior to 2.2.0.	9.8	More Details
CVE-2022-36267	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists a Unauthenticated remote command injection vulnerability. The ping functionality can be called without user authentication when crafting a malicious http request by injecting code in one of the parameters allowing for remote code execution. This vulnerability is exploited via the binary file /home/www/cgi-bin/diagnostics.cgi that accepts unauthenticated requests and unsanitized data. As a result, a malicious actor can craft a specific request and interact remotely with the device.	9.8	More Details
CVE-2021-41615	websda.c in GoAhead WebServer 2.1.8 has insufficient nonce entropy because the nonce calculation relies on the hardcoded onceuponatimeinparadise value, which does not follow the secret-data guideline for HTTP Digest Access Authentication in RFC 7616 section 3.3 (or RFC 2617 section 3.2.1). NOTE: 2.1.8 is a version from 2003; however, the affected websda.c code appears in multiple derivative works that may be used in 2021. Recent GoAhead software is unaffected.	9.8	More Details
CVE-2022-30133	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability	9.8	More Details
CVE-2022-24015	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the log_upload binary.	9.8	More Details
CVE-2022-24014	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the logserver binary.	9.8	More Details
CVE-2022-24013	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the gpio_ctrl binary.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32964	OMICARD EDM's API function has insufficient validation for user input. An unauthenticated remote attacker can inject arbitrary SQL commands to access, modify, delete database or disrupt service.	9.8	More Details
CVE-2022-21186	The package @acrontum/filesystem-template before 0.0.2 are vulnerable to Arbitrary Command Injection due to the fetchRepo API missing sanitization of the href field of external input.	9.8	More Details
CVE-2022-35143	Renato v0.17.0 employs weak password complexity requirements, allowing attackers to crack user passwords via brute-force attacks.	9.8	More Details
CVE-2022-34993	Totolink A3600R_Firmware V4.1.2cu.5182_B20201102 contains a hard code password for root in /etc/shadow.sample.	9.8	More Details
CVE-2022-34970	Crow before 1.0+4 has a heap-based buffer overflow via the function qs_parse in query_string.h. On successful exploitation this vulnerability allows attackers to remotely execute arbitrary code in the context of the vulnerable service.	9.8	More Details
CVE-2022-25168	Apache Hadoop's FileUtil.unTar(File, File) API does not escape the input file name before being passed to the shell. An attacker can inject arbitrary commands. This is only used in Hadoop 3.3 InMemoryAliasMap.completeBootstrapTransfer, which is only ever run by a local user. It has been used in Hadoop 2.x for yarn localization, which does enable remote code execution. It is used in Apache Spark, from the SQL command ADD ARCHIVE. As the ADD ARCHIVE command adds new binaries to the classpath, being able to execute shell scripts does not confer new permissions to the caller. SPARK-38305. "Check existence of file before untarring/zipping", which is included in 3.3.0, 3.1.4, 3.2.2, prevents shell commands being executed, regardless of which version of the hadoop libraries are in use. Users should upgrade to Apache Hadoop 2.10.2, 3.2.4, 3.3.3 or upper (including HADOOP-18136).	9.8	More Details
CVE-2022-32965	OMICARD EDM has a hard-coded machine key. An unauthenticated remote attacker can use the machine key to send serialized payload to the server to execute arbitrary code, manipulate system data and disrupt service.	9.8	More Details
CVE-2022-2651	Authentication Bypass by Primary Weakness in GitHub repository bookwyrm-social/bookwyrm prior to 0.4.5.	9.8	More Details
CVE-2022-31656	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate.	9.8	More Details
CVE-2022-35161	GVRET Stable Release as of Aug 15, 2015 was discovered to contain a buffer overflow via the handleConfigCmd function at SerialConsole.cpp.	9.8	More Details
CVE-2022-35866	This vulnerability allows remote attackers to bypass authentication on affected installations of Vinchin Backup and Recovery 6.5.0.17561. Authentication is not required to exploit this vulnerability. The specific flaw exists within the configuration of the MySQL server. The server uses a hard-coded password for the administrator user. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-17139.	9.8	More Details
CVE-2022-35865	This vulnerability allows remote attackers to execute arbitrary code on affected installations of BMC Track-It! 20.21.2.109. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authorization of HTTP requests. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16709.	9.8	More Details
CVE-2022-2272	This vulnerability allows remote attackers to bypass authentication on affected installations of Sante PACS Server 3.0.4. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of calls to the login endpoint. When parsing the username element, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-17331.	9.8	More Details
CVE-2022-35620	D-LINK DIR-818LW A1:DIR818L_FW105b01 was discovered to contain a remote code execution (RCE) vulnerability via the function binary.soapcgi_main.	9.8	More Details
CVE-2022-35619	D-LINK DIR-818LW A1:DIR818L_FW105b01 was discovered to contain a remote code execution (RCE) vulnerability via the function ssdpcgi_main.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24012	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the fota binary.	9.8	More Details
CVE-2022-37434	zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference).	9.8	More Details
CVE-2022-31657	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain.	9.8	More Details
CVE-2022-24005	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the ap_steer binary.	9.8	More Details
CVE-2022-24011	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the device_list binary.	9.8	More Details
CVE-2022-24010	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the cwmpd binary.	9.8	More Details
CVE-2022-24009	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the confsrv binary.	9.8	More Details
CVE-2022-24008	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the confcli binary.	9.8	More Details
CVE-2022-24007	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the cfm binary.	9.8	More Details
CVE-2022-21178	An os command injection vulnerability exists in the confsrv ucloud_add_new_node functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to arbitrary command execution. An attacker can send a malicious packet to trigger this vulnerability.	9.8	More Details
CVE-2022-24006	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the arpbrocast binary.	9.8	More Details
CVE-2022-23919	A stack-based buffer overflow vulnerability exists in the confsrv set_mf_rule functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.This vulnerability leverages the name field within the protobuf message to cause a buffer overflow.	9.8	More Details
CVE-2022-23918	A stack-based buffer overflow vulnerability exists in the confsrv set_mf_rule functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.This vulnerability leverages the ethAddr field within the protobuf message to cause a buffer overflow.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23399	A stack-based buffer overflow vulnerability exists in the confsrv set_port_fwd_rule functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.	9.8	More Details
CVE-2022-23103	A stack-based buffer overflow vulnerability exists in the confsrv confctl_set_app_language functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.	9.8	More Details
CVE-2022-22144	A hard-coded password vulnerability exists in the libcommonprod.so prod_change_root_passwd functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. During system startup this functionality is always called, leading to a known root password. An attacker does not have to do anything to trigger this vulnerability.	9.8	More Details
CVE-2022-22140	An os command injection vulnerability exists in the confsrv ucloud_add_node functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to arbitrary command execution. An attacker can send a malicious packet to trigger this vulnerability.	9.8	More Details
CVE-2022-34715	Windows Network File System Remote Code Execution Vulnerability	9.8	More Details
CVE-2022-33649	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	9.6	More Details
CVE-2022-36264	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists an Unauthenticated remote Arbitrary File Upload vulnerability which allows overwriting arbitrary files. A malicious actor can remotely upload a file of their choice and overwrite any file in the system by manipulating the filename and append a relative path that will be interpreted during the upload process. Using this method, it is possible to rewrite any file in the system or upload a new file.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-34717	Microsoft Office Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-34928	JFinal CMS v5.1.0 was discovered to contain a SQL injection vulnerability via /system/user.	8.8	More Details
CVE-2022-35777	Visual Studio Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-24023	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the pppd binary.	8.8	More Details
CVE-2022-28684	This vulnerability allows remote attackers to execute arbitrary code on affected installations of DevExpress. Authentication is required to exploit this vulnerability. The specific flaw exists within the SafeBinaryFormatter library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16710.	8.8	More Details
CVE-2022-36359	An issue was discovered in the HTTP FileResponse class in Django 3.2 before 3.2.15 and 4.0 before 4.0.7. An application is vulnerable to a reflected file download (RFD) attack that sets the Content-Disposition header of a FileResponse when the filename is derived from user-supplied input.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34691	Active Directory Domain Services Elevation of Privilege Vulnerability	8.8	More Details
CVE-2022-2356	The Frontend File Manager & Sharing WordPress plugin before 1.1.3 does not filter file extensions when letting users upload files on the server, which may lead to malicious code being uploaded.	8.8	More Details
CVE-2022-34158	A carefully crafted invocation on the Image plugin could trigger an CSRF vulnerability on Apache JSPWiki before 2.11.3, which could allow a group privilege escalation of the attacker's account. Further examination of this issue established that it could also be used to modify the email associated with the attacked account, and then a reset password request from the login page.	8.8	More Details
CVE-2022-35804	SMB Client and Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-21201	A stack-based buffer overflow vulnerability exists in the confers ucloud_add_node_new functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.	8.8	More Details
CVE-2022-35826	Visual Studio Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-35825	Visual Studio Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-34937	Yuba u5cms v8.3.5 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component savepage.php. This vulnerability allows attackers to execute arbitrary code.	8.8	More Details
CVE-2022-35827	Visual Studio Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-35243	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2022-33719	Improper input validation in baseband prior to SMR Aug-2022 Release 1 allows attackers to cause integer overflow to heap overflow.	8.6	More Details
CVE-2022-2636	Improper Control of Generation of Code ('Code Injection') in GitHub repository hestiacp/hestiacp prior to 1.6.6.	8.5	More Details
CVE-2022-2497	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.6 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. A malicious developer could exfiltrate an integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server.	8.5	More Details
CVE-2022-35928	AES Crypt is a file encryption software for multiple platforms. AES Crypt for Linux built using the source on GitHub and having the version number 3.11 has a vulnerability with respect to reading user-provided passwords and confirmations via command-line prompts. Passwords lengths were not checked before being read. This vulnerability may lead to buffer overruns. This does _not_ affect source code found on aescrypt.com, nor is the vulnerability present when providing a password or a key via the `-p` or `-k` command-line options. The problem was fixed via in commit 68761851b and will be included in release 3.16. Users are advised to upgrade. Users unable to upgrade should us the `-p` or `-k` options to provide a password or key.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31132	Nextcloud Mail is an email application for the nextcloud personal cloud product. Affected versions shipped with a CSS minifier on the path `./vendor/cerdic/css-tidy/css_optimiser.php`. Access to the minifier is unrestricted and access may lead to Server-Side Request Forgery (SSRF). It is recommendet to upgrade to Mail 1.12.7 or Mail 1.13.6. Users unable to upgrade may manually delete the file located at `./vendor/cerdic/css-tidy/css_optimiser.php`	8.3	More Details
CVE-2022-33636	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	8.3	More Details
CVE-2022-2732	Missing Authorization in GitHub repository openemr/openemr prior to 7.0.0.1.	8.3	More Details
CVE-2022-35936	Ethermint is an Ethereum library. In Ethermint running versions before `v0.17.2`, the contract `selfdestruct` invocation permanently removes the corresponding bytecode from the internal database storage. However, due to a bug in the `DeleteAccount`function, all contracts that used the identical bytecode (i.e shared the same `CodeHash`) will also stop working once one contract invokes `selfdestruct`, even though the other contracts did not invoke the `selfdestruct` OPCODE. This vulnerability has been patched in Ethermint version v0.18.0. The patch has state machine-breaking changes for applications using Ethermint, so a coordinated upgrade procedure is required. A workaround is available. If a contract is subject to DoS due to this issue, the user can redeploy the same contract, i.e. with identical bytecode, so that the original contract's code is recovered. The new contract deployment restores the `bytecode hash -> bytecode` entry in the internal state.	8.2	More Details
CVE-2022-1012	A memory leak problem was found in the TCP source port generation algorithm in net/ipv4/tcp.c due to the small table perturb size. This flaw may allow an attacker to information leak and may cause a denial of service problem.	8.2	More Details
CVE-2022-34702	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-34714	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-35767	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-35728	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2022-35766	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2021-32771	Contiki-NG is an open-source, cross-platform operating system for IoT devices. In affected versions it is possible to cause a buffer overflow when copying an IPv6 address prefix in the RPL-Classic implementation in Contiki-NG. In order to trigger the vulnerability, the Contiki-NG system must have joined an RPL DODAG. After that, an attacker can send a DAO packet with a Target option that contains a prefix length larger than 128 bits. The problem was fixed after the release of Contiki-NG 4.7. Users unable to upgrade may apply the patch in Contiki-NG PR #1615.	8.1	More Details
CVE-2022-35927	Contiki-NG is an open-source, cross-platform operating system for IoT devices. In the RPL-Classic routing protocol implementation in the Contiki-NG operating system, an incoming DODAG Information Option (DIO) control message can contain a prefix information option with a length parameter. The value of the length parameter is not validated, however, and it is possible to cause a buffer overflow when copying the prefix in the set_ip_from_prefix function. This vulnerability affects anyone running a Contiki-NG version prior to 4.7 that can receive RPL DIO messages from external parties. To obtain a patched version, users should upgrade to Contiki-NG 4.7 or later. There are no workarounds for this issue.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32293	In ConnMan through 1.41, a man-in-the-middle attack against a WISPR HTTP query could be used to trigger a use-after-free in WISPR handling, leading to crashes or code execution.	8.1	More Details
CVE-2022-35794	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-35802	Azure Site Recovery Elevation of Privilege Vulnerability	8.1	More Details
CVE-2022-24477	Microsoft Exchange Server Elevation of Privilege Vulnerability	8.0	More Details
CVE-2022-24516	Microsoft Exchange Server Elevation of Privilege Vulnerability	8.0	More Details
CVE-2022-21980	Microsoft Exchange Server Elevation of Privilege Vulnerability	8.0	More Details
CVE-2022-33648	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-30176	Azure RTOS GUIX Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-34707	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-34706	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-34705	Windows Defender Credential Guard Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-34703	Windows Partition Management Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-34696	Windows Hyper-V Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-34699	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-35858	The TEE_PopulateTransientObject and __utee_from_attr functions in Samsung mTower 0.3.0 allow a trusted application to trigger a memory overwrite, denial of service, and information disclosure by invoking the function TEE_PopulateTransientObject with a large number in the parameter attrCount.	7.8	More Details
CVE-2022-33640	System Center Operations Manager: Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34687	Azure RTOS GUIX Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-33670	Windows Partition Management Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-37415	The Uniwill SparkIO.sys driver 1.0 is vulnerable to a stack-based buffer overflow via IOCTL 0x40002008.	7.8	More Details
CVE-2022-37030	Weak permissions on the configuration file in the PAM module in Grommunio Gromox 0.5 through 1.x before 1.28 allow a local unprivileged user in the gromox group to have the PAM stack execute arbitrary code upon loading the Gromox PAM module.	7.8	More Details
CVE-2022-34713	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-34927	MilkyTracker v1.03.00 was discovered to contain a stack overflow via the component LoaderXM::load. This vulnerability is triggered when the program is supplied a crafted XM module file.	7.8	More Details
CVE-2022-32543	An integer overflow vulnerability exists in the way ESTsoft Alyac 2.5.8.544 parses OLE files. A specially-crafted OLE file can lead to a heap buffer overflow which can result in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-35795	Windows Error Reporting Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-34992	Luadec v0.9.9 was discovered to contain a heap-buffer overflow via the function UnsetPending.	7.8	More Details
CVE-2022-35779	Azure RTOS GUIX Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-35792	Storage Spaces Direct Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-31660	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'.	7.8	More Details
CVE-2022-31661	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'.	7.8	More Details
CVE-2022-28668	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 11.9.2. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16679.	7.8	More Details
CVE-2022-31664	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35771	Windows Defender Credential Guard Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-31609	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it allows the guest VM to allocate resources for which the guest is not authorized. This vulnerability may lead to loss of data integrity and confidentiality, denial of service, or information disclosure.	7.8	More Details
CVE-2022-35806	Azure RTOS GUIX Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-35820	Windows Bluetooth Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-22299	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments.	7.8	More Details
CVE-2022-27535	Kaspersky VPN Secure Connection for Windows version up to 21.5 was vulnerable to arbitrary file deletion via abuse of its 'Delete All Service Data And Reports' feature by the local authenticated attacker.	7.8	More Details
CVE-2022-1158	A flaw was found in KVM. When updating a guest's page table entry, vm_pgoff was improperly used as the offset to get the page's pfn. As vaddr and vm_pgoff are controllable by user-mode processes, this flaw allows unprivileged local users on the host to write outside the userspace region and potentially corrupt the kernel, resulting in a denial of service condition.	7.8	More Details
CVE-2022-35773	Azure RTOS GUIX Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-30175	Azure RTOS GUIX Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-35768	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-35760	Microsoft ATA Port Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-29886	An integer overflow vulnerability exists in the way ESTsoft Alyac 2.5.8.544 parses OLE files. A specially-crafted OLE file can lead to a heap buffer overflow, which can result in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-35761	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-35762	Storage Spaces Direct Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-35763	Storage Spaces Direct Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35764	Storage Spaces Direct Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-35765	Storage Spaces Direct Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-1704	Due to an XML external entity reference, the software parses XML in the backup/restore functionality without XML security flags, which may lead to a XXE attack while restoring the backup.	7.6	More Details
CVE-2022-37451	Exim before 4.96 has an invalid free in pam_converse in auths/call_pam.c because store_free is not used after store_malloc.	7.5	More Details
CVE-2022-27944	Foxit PDF Reader before 12.0.1 and PDF Editor before 12.0.1 allow an exportXFAData NULL pointer dereference.	7.5	More Details
CVE-2022-26979	Foxit PDF Reader before 12.0.1 and PDF Editor before 12.0.1 allow a NULL pointer dereference when this.Span is used for oState of Collab.addStateModel, because this.Span.text can be NULL.	7.5	More Details
CVE-2022-31662	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files.	7.5	More Details
CVE-2022-36125	It is possible to crash (panic) an application by providing a corrupted data to be read. This issue affects Rust applications using Apache Avro Rust SDK prior to 0.14.0 (previously known as avro-rs). Users should update to apache-avro version 0.14.0 which addresses this issue.	7.5	More Details
CVE-2022-35487	Zammad 5.2.0 suffers from Incorrect Access Control. Zammad did not correctly perform authorization on certain attachment endpoints. This could be abused by an unauthenticated attacker to gain access to attachments, such as emails or attached files.	7.5	More Details
CVE-2022-36124	It is possible for a Reader to consume memory beyond the allowed constraints and thus lead to out of memory on the system. This issue affects Rust applications using Apache Avro Rust SDK prior to 0.14.0 (previously known as avro-rs). Users should update to apache-avro version 0.14.0 which addresses this issue.	7.5	More Details
CVE-2022-2357	The WSM Downloader WordPress plugin through 1.4.0 allows any visitor to use its remote file download feature to download any local files, including sensitive ones like wp-config.php.	7.5	More Details
CVE-2022-27660	A denial of service vulnerability exists in the confctl_set_guest_wlan functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to trigger this vulnerability.	7.5	More Details
CVE-2022-2367	The WSM Downloader WordPress plugin through 1.4.0 allows only specific popular websites to download images/files from, this can be bypassed due to the lack of good "link" parameter validation	7.5	More Details
CVE-2022-35724	It is possible to provide data to be read that leads the reader to loop in cycles endlessly, consuming CPU. This issue affects Rust applications using Apache Avro Rust SDK prior to 0.14.0 (previously known as avro-rs). Users should update to apache-avro version 0.14.0 which addresses this issue.	7.5	More Details
CVE-2022-25907	The package ts-deepmerge before 2.0.2 are vulnerable to Prototype Pollution due to missing sanitization of the merge function.	7.5	More Details
CVE-2022-34293	wolfSSL before 5.4.0 allows remote attackers to cause a denial of service via DTLS because a check for return-routability can be skipped.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2053	When a POST request comes through AJP and the request exceeds the max-post-size limit (maxEntitySize), Undertow's AjpServerRequestConduit implementation closes a connection without sending any response to the client/proxy. This behavior results in that a front-end proxy marking the backend worker (application server) as an error state and not forward requests to the worker for a while. In mod_cluster, this continues until the next STATUS request (10 seconds intervals) from the application server updates the server state. So, in the worst case, it can result in "All workers are in error state" and mod_cluster responds "503 Service Unavailable" for a while (up to 10 seconds). In mod_proxy_balancer, it does not forward requests to the worker until the "retry" timeout passes. However, luckily, mod_proxy_balancer has "forcerecovery" setting (On by default; this parameter can force the immediate recovery of all workers without considering the retry parameter of the workers if all workers of a balancer are in error state.). So, unlike mod_cluster, mod_proxy_balancer does not result in responding "503 Service Unavailable". An attacker could use this behavior to send a malicious request and trigger server errors, resulting in DoS (denial of service). This flaw was fixed in Undertow 2.2.19.Final, Undertow 2.3.0.Alpha2.	7.5	More Details
CVE-2022-30144	Windows Bluetooth Service Remote Code Execution Vulnerability	7.5	More Details
CVE-2022-27633	An information disclosure vulnerability exists in the confctl_get_guest_wlan functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to information disclosure. An attacker can send packets to trigger this vulnerability.	7.5	More Details
CVE-2022-27185	A denial of service vulnerability exists in the confctl_set_master_wlan functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to trigger this vulnerability.	7.5	More Details
CVE-2022-27630	An information disclosure vulnerability exists in the confctl_get_master_wlan functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to information disclosure. An attacker can send packets to trigger this vulnerability.	7.5	More Details
CVE-2022-35488	In Zammad 5.2.0, an attacker could manipulate the rate limiting in the 'forgot password' feature of Zammad, and thereby send many requests for a known account to cause Denial Of Service by many generated emails which would also spam the victim.	7.5	More Details
CVE-2022-35245	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5.1, when a BIG-IP APM access policy is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2022-32963	OMICARD EDM’s mail file relay function has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to by-pass authentication and access arbitrary system files.	7.5	More Details
CVE-2022-35240	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2022-35216	OMICARD EDM’s mail image relay function has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to by-pass authentication and access arbitrary system files.	7.5	More Details
CVE-2022-32455	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2022-33203	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when a BIG-IP APM access policy with Service Connect agent is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34701	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability	7.5	More Details
CVE-2022-35506	TripleCross v0.1.0 was discovered to contain a stack overflow which occurs because there is no limit to the length of program parameters.	7.5	More Details
CVE-2022-34651	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2022-34655	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2022-35505	A segmentation fault in TripleCross v0.1.0 occurs when sending a control command from the client to the server. This occurs because there is no limit to the length of the output of the executed command.	7.5	More Details
CVE-2022-34862	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2022-35236	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2022-35158	A vulnerability in the lua parser of TscanCode tsclua v2.15.01 allows attackers to cause a Denial of Service (DoS) via a crafted lua script.	7.5	More Details
CVE-2022-35272	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2022-35769	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability	7.5	More Details
CVE-2022-34973	D-Link DIR820LA1_FW106B02 was discovered to contain a buffer overflow via the nextPage parameter at ping.ccp.	7.5	More Details
CVE-2022-35142	An issue in Renato v0.17.0 allows attackers to cause a Denial of Service (DoS) via a crafted payload injected into the Search parameter.	7.5	More Details
CVE-2022-35796	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	7.5	More Details
CVE-2022-31793	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected.	7.5	More Details
CVE-2022-35737	SQLite 1.0.12 through 3.39.x before 3.39.2 sometimes allows an array-bounds overflow if billions of bytes are used in a string argument to a C API.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34969	PingCAP TiDB v6.1.0 was discovered to contain a NULL pointer dereference.	7.5	More Details
CVE-2022-34968	An issue in the fetch_step function in Percona Server for MySQL v8.0.28-19 allows attackers to cause a Denial of Service (DoS) via a SQL query.	7.5	More Details
CVE-2022-34967	The assertion `stmt->Dbc->FirstStmt' failed in MonetDB Database Server v11.43.13.	7.5	More Details
CVE-2022-30194	Windows WebBrowser Control Remote Code Execution Vulnerability	7.5	More Details
CVE-2022-2647	A vulnerability was found in jeecg-boot. It has been declared as critical. This vulnerability affects unknown code of the file /api/. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-205594 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2022-35793	Windows Print Spooler Elevation of Privilege Vulnerability	7.3	More Details
CVE-2022-2674	A vulnerability was found in SourceCodester Best Fee Management System. It has been rated as critical. Affected by this issue is the function login of the file admin_class.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-205658 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2022-2702	A vulnerability was found in SourceCodester Company Website CMS and classified as critical. Affected by this issue is some unknown functionality of the file site-settings.php of the component Cookie Handler. The manipulation leads to improper access controls. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-205826 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2022-2664	A vulnerability classified as critical has been found in Private Cloud Management Platform. Affected is an unknown function of the file /management/api/rcx_management/global_config_query of the component POST Request Handler. The manipulation leads to improper authentication. It is possible to launch the attack remotely. VDB-205614 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2022-33631	Microsoft Excel Security Feature Bypass Vulnerability	7.3	More Details
CVE-2022-36833	Improper Privilege Management vulnerability in Game Optimizing Service prior to versions 3.3.04.0 in Android 10, and 3.5.04.8 in Android 11 and above allows local attacker to execute hidden function for developer by changing package name.	7.3	More Details
CVE-2022-35772	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-31658	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution.	7.2	More Details
CVE-2022-31659	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution.	7.2	More Details
CVE-2022-35735	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34871	This vulnerability allows remote attackers to escalate privileges on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the configuration of poller resources. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to the level of an administrator. Was ZDI-CAN-16335.	7.2	More Details
CVE-2022-27616	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in webapi component in Synology DiskStation Manager (DSM) before 7.0.1-42218-3 allows remote authenticated users to execute arbitrary commands via unspecified vectors.	7.2	More Details
CVE-2022-36265	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists a Hidden system command web page. After performing a reverse engineering of the firmware, it was discovered that a hidden page not listed in the administration management interface allows a user to execute Linux commands on the device with root privileges. An authenticated malicious threat actor can use this page to fully compromise the device.	7.2	More Details
CVE-2022-31665	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution.	7.2	More Details
CVE-2022-2668	An issue was discovered in Keycloak that allows arbitrary Javascript to be uploaded for the SAML protocol mapper even if the UPLOAD_SCRIPTS feature is disabled	7.2	More Details
CVE-2022-35824	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-2626	Incorrect Privilege Assignment in GitHub repository hestiacp/hestiacp prior to 1.6.6.	7.2	More Details
CVE-2022-37398	A stack-based buffer overflow vulnerability was found inside ADM when using WebDAV due to the lack of data size validation. An attacker can exploit this vulnerability to run arbitrary code. Affected ADM versions include: 3.5.9.RUE3 and below, 4.0.5.RVI1 and below as well as 4.1.0.RJD1 and below.	7.1	More Details
CVE-2022-1973	A use-after-free flaw was found in the Linux kernel in log_replay in fs/ntfs3/fslog.c in the NTFS journal. This flaw allows a local attacker to crash the system and leads to a kernel information leak problem.	7.1	More Details
CVE-2022-35930	PolicyController is a utility used to enforce supply chain policy in Kubernetes clusters. In versions prior to 0.2.1 PolicyController will report a false positive, resulting in an admission when it should not be admitted when there is at least one attestation with a valid signature and there are NO attestations of the type being verified (--type defaults to "custom"). An example image that can be used to test this is `ghcr.io/distroless/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e2`. Users should upgrade to version 0.2.1 to resolve this issue. There are no workarounds for users unable to upgrade.	7.1	More Details
CVE-2022-31197	PostgreSQL JDBC Driver (PgJDBC for short) allows Java programs to connect to a PostgreSQL database using standard, database independent Java code. The PGJDBC implementation of the `java.sql.ResultRow.refreshRow()` method is not performing escaping of column names so a malicious column name that contains a statement terminator, e.g. `;`, could lead to SQL injection. This could lead to executing additional SQL commands as the application's JDBC user. User applications that do not invoke the `ResultSet.refreshRow()` method are not impacted. User application that do invoke that method are impacted if the underlying database that they are querying via their JDBC application may be under the control of an attacker. The attack requires the attacker to trick the user into executing SQL against a table name who's column names would contain the malicious SQL and subsequently invoke the `refreshRow()` method on the ResultSet. Note that the application's JDBC user and the schema owner need not be the same. A JDBC application that executes as a privileged user querying database schemas owned by potentially malicious less-privileged users would be vulnerable. In that situation it may be possible for the malicious user to craft a schema that causes the application to execute commands as the privileged user. Patched versions will be released as `42.2.26` and `42.4.1`. Users are advised to upgrade. There are no known workarounds for this issue.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34690	Windows Fax Service Elevation of Privilege Vulnerability	7.1	More Details
CVE-2022-35929	cosign is a container signing and verification utility. In versions prior to 1.10.1 cosign can report a false positive if any attestation exists. `cosign verify-attestation` used with the `--type` flag will report a false positive verification when there is at least one attestation with a valid signature and there are NO attestations of the type being verified (--type defaults to "custom"). This can happen when signing with a standard keypair and with "keyless" signing with Fulcio. This vulnerability can be reproduced with the `distroless.dev/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e2` image. This image has a `vuln` attestation but not an `spdx` attestation. However, if you run `cosign verify-attestation --type=spdx` on this image, it incorrectly succeeds. This issue has been addressed in version 1.10.1 of cosign. Users are advised to upgrade. There are no known workarounds for this issue.	7.1	More Details
CVE-2022-31614	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin) where it may double-free some resources. An attacker may exploit this vulnerability with other vulnerabilities to cause denial of service, code execution, and information disclosure.	7.0	More Details
CVE-2022-33646	Azure Batch Node Agent Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-33730	Heap-based buffer overflow vulnerability in Samsung Dex for PC prior to SMR Aug-2022 Release 1 allows arbitrary code execution by physical attackers.	6.8	More Details
CVE-2022-29083	Prior Dell BIOS versions contain an Improper Authentication vulnerability. An unauthenticated attacker with physical access to the system could potentially exploit this vulnerability by bypassing drive security mechanisms in order to gain access to the system.	6.8	More Details
CVE-2022-27619	Cleartext transmission of sensitive information vulnerability in authentication management in Synology Note Station Client before 2.2.2-609 allows man-in-the-middle attackers to obtain sensitive information via unspecified vectors.	6.8	More Details
CVE-2022-27620	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology SSO Server before 2.2.3-0331 allows remote authenticated users to read arbitrary files via unspecified vectors.	6.8	More Details
CVE-2022-31473	In BIG-IP Versions 16.1.x before 16.1.1 and 15.1.x before 15.1.4, when running in Appliance mode, an authenticated attacker may be able to bypass Appliance mode restrictions due to a directory traversal vulnerability in an undisclosed page within iApps. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.8	More Details
CVE-2022-27618	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology Storage Analyzer before 2.1.0-0390 allows remote authenticated users to delete arbitrary files via unspecified vectors.	6.8	More Details
CVE-2022-35867	This vulnerability allows local attackers to escalate privileges on affected installations of xhyve. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the e1000 virtual device. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-15056.	6.7	More Details
CVE-2022-33962	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30573	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, and TIBCO FTL - Enterprise Edition contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a privilege escalation on the affected ftlserver. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO FTL - Enterprise Edition: version 6.8.0.	6.7	More Details
CVE-2022-35489	In Zammad 5.2.0, customers who have secondary organizations assigned were able to see all organizations of the system rather than only those to which they are assigned.	6.5	More Details
CVE-2022-2512	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.0 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. Membership changes are not reflected in TODO for confidential notes, allowing a former project members to read updates via TODOs.	6.5	More Details
CVE-2022-35818	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-28731	A carefully crafted request on UserPreferences.jsp could trigger an CSRF vulnerability on Apache JSPWiki before 2.11.3, which could allow the attacker to modify the email associated with the attacked account, and then a reset password request from the login page.	6.5	More Details
CVE-2022-2653	With this vulnerability an attacker can read many sensitive files like configuration files, or the /proc/self/environ file, that contains the environment variable used by the web server that includes database credentials. If the web server user is root, an attacker will be able to read any file in the system.	6.5	More Details
CVE-2022-31118	Nextcloud server is an open source personal cloud solution. In affected versions an attacker could brute force to find if federated sharing is being used and potentially try to brute force access tokens for federated shares (`a-zA-Z0-9` ^ 15). It is recommended that the Nextcloud Server is upgraded to 22.2.9, 23.0.6 or 24.0.2. Users unable to upgrade may disable federated sharing via the Admin Sharing settings in `index.php/settings/admin/sharing`.	6.5	More Details
CVE-2022-35799	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35817	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35241	In versions 2.x before 2.3.1 and all versions of 1.x, when NGINX Instance Manager is in use, undisclosed requests can cause an increase in disk resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2022-37416	Ittiam libmpeg2 before 2022-07-27 uses memcpy with overlapping memory blocks in impeg2_mc_fullx_fully_8x8.	6.5	More Details
CVE-2022-35801	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-30134	Microsoft Exchange Server Information Disclosure Vulnerability	6.5	More Details
CVE-2022-35816	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-2730	Authorization Bypass Through User-Controlled Key in GitHub repository openemr/openemr prior to 7.0.0.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1323	The Discy WordPress theme before 5.0 lacks authorization checks then processing ajax requests to the discy_update_options action, allowing any logged in users (with privileges as low as Subscriber,) to change Theme options by sending a crafted POST request.	6.5	More Details
CVE-2022-2355	The Easy Username Updater WordPress plugin before 1.0.5 does not implement CSRF checks, which could allow attackers to make a logged in admin change any user's username includes the admin	6.5	More Details
CVE-2022-35807	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35808	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35809	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35810	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35811	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35813	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35814	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35815	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-2675	Using off-the-shelf commodity hardware, the Unitree Go 1 robotics platform version H0.1.7 and H0.1.9 (using firmware version 0.1.35) can be powered down by an attacker within normal RF range without authentication. Other versions may be affected, such as the A1.	6.5	More Details
CVE-2022-30535	In versions 2.x before 2.3.0 and all versions of 1.x, An attacker authorized to create or update ingress objects can obtain the secrets available to the NGINX Ingress Controller. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2022-35786	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35781	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-34872	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of Virtual Metrics. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-16336.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35819	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35775	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35864	This vulnerability allows remote attackers to disclose sensitive information on affected installations of BMC Track-It! 20.21.02.109. Authentication is required to exploit this vulnerability. The specific flaw exists within the GetPopupSubQueryDetails endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-16690.	6.5	More Details
CVE-2022-34768	insert HTML / js code inside input how to get to the vulnerable input : Workers > worker nickname > inject in this input the code.	6.5	More Details
CVE-2022-35785	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-36296	Broken Authentication vulnerability in JumpDEMAND Inc. ActiveDEMAND plugin <= 0.2.27 at WordPress allows unauthenticated post update/create/delete.	6.5	More Details
CVE-2022-35784	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35788	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35791	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35789	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35790	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35782	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-35780	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-2498	An issue in pipeline subscriptions in GitLab EE affecting all versions from 12.8 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 triggered new pipelines with the person who created the tag as the pipeline creator instead of the subscription's author.	6.4	More Details
CVE-2022-2326	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible to gain access to a private project through an email invite by using other user's email address as an unverified secondary email.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36284	Authenticated IDOR vulnerability in StoreApps Affiliate For WooCommerce premium plugin <= 4.7.0 at WordPress allows an attacker to change the PayPal email. WooCommerce PayPal Payments plugin (free) should be at least installed to get the extra input field on the user profile page.	6.4	More Details
CVE-2022-2698	A vulnerability was found in SourceCodester Simple E-Learning System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file search.php. The manipulation of the argument searchPost leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205819.	6.3	More Details
CVE-2022-2697	A vulnerability was found in SourceCodester Simple E-Learning System. It has been classified as critical. Affected is an unknown function of the file comment_frame.php. The manipulation of the argument post_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-205818 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-2699	A vulnerability was found in SourceCodester Simple E-Learning System. It has been rated as critical. Affected by this issue is some unknown functionality of the file /claire_blake. The manipulation of the argument phoneNumber leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-205820.	6.3	More Details
CVE-2022-2723	A vulnerability was found in SourceCodester Employee Management System. It has been classified as critical. Affected is an unknown function of the file /process/eprocess.php. The manipulation of the argument mailuid/pwd leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-205836.	6.3	More Details
CVE-2022-2694	A vulnerability was found in SourceCodester Company Website CMS and classified as critical. This issue affects some unknown processing. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205817 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2665	A vulnerability classified as critical was found in SourceCodester Simple E-Learning System. Affected by this vulnerability is an unknown functionality of the file classroom.php. The manipulation of the argument post_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205615.	6.3	More Details
CVE-2022-2726	A vulnerability classified as critical has been found in SEMCMS. This affects an unknown part of the file Ant_Check.php. The manipulation of the argument DID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205839.	6.3	More Details
CVE-2022-2724	A vulnerability was found in SourceCodester Employee Management System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /process/aprocess.php. The manipulation of the argument mailuid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205837 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2722	A vulnerability was found in SourceCodester Simple Student Information System and classified as critical. This issue affects some unknown processing of the file manage_course.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205835.	6.3	More Details
CVE-2022-2703	A vulnerability was found in SourceCodester Gym Management System. It has been classified as critical. This affects an unknown part of the component Exercises Module. The manipulation of the argument exer leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205827.	6.3	More Details
CVE-2022-34769	Michlol - rashim web interface Insecure direct object references (IDOR). First of all, the attacker needs to login. After he performs log into the system there are some functionalities that the specific user is not allowed to perform. However all the attacker needs to do in order to achieve his goals is to change the value of the ptMsl parameter and then the attacker can access sensitive data that he not supposed to access because its belong to another user.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2705	A vulnerability was found in SourceCodester Simple Student Information System. It has been rated as critical. This issue affects some unknown processing of the file admin/departments/manage_department.php. The manipulation of the argument id with the input -5756%27%20UNION%20ALL%20SELECT%20NULL,database(),user(),NULL,NULL,NULL,NULL--%20- leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205829 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2706	A vulnerability classified as critical has been found in SourceCodester Online Class and Exam Scheduling System 1.0. Affected is an unknown function of the file /pages/class_sched.php. The manipulation of the argument class with the input 'll(SELECT 0x684d6b6c WHERE 5993=5993 AND (SELECT 2096 FROM(SELECT COUNT(*),CONCAT(0x717a786b71,(SELECT (ELT(2096=2096,1))),0x717a626271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))ll' leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-205830 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-2707	A vulnerability classified as critical was found in SourceCodester Online Class and Exam Scheduling System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/faculty_sched.php. The manipulation of the argument faculty with the input ' OR (SELECT 2078 FROM(SELECT COUNT(*),CONCAT(0x716a717071,(SELECT (ELT(2078=2078,1))),0x717a706a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- uYCM leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205831.	6.3	More Details
CVE-2022-2728	A vulnerability was found in SourceCodester Gym Management System. It has been rated as critical. Affected by this issue is some unknown functionality of the file /mygym/admin/index.php. The manipulation of the argument edit_tran leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-205856.	6.3	More Details
CVE-2022-2693	A vulnerability has been found in SourceCodester Electronic Medical Records System and classified as critical. This vulnerability affects unknown code of the file register.php of the component UPDATE Statement Handler. The manipulation of the argument pconsultation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-205816.	6.3	More Details
CVE-2022-2727	A vulnerability was found in SourceCodester Gym Management System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /mygym/admin/login.php. The manipulation of the argument admin_email/admin_pass leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205855.	6.3	More Details
CVE-2022-2673	A vulnerability was found in Rigatur Online Booking and Hotel Management System aff6409. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file login.php of the component POST Request Handler. The manipulation of the argument email/pass leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205657 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2672	A vulnerability was found in SourceCodester Garage Management System. It has been classified as critical. Affected is an unknown function of the file createUser.php. The manipulation of the argument userName/uemail leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-205656.	6.3	More Details
CVE-2022-2676	A vulnerability was found in SourceCodester Electronic Medical Records System and classified as critical. Affected by this issue is some unknown functionality of the component POST Request Handler. The manipulation of the argument user_email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-205664.	6.3	More Details
CVE-2022-2677	A vulnerability was found in SourceCodester Apartment Visitor Management System 1.0. It has been classified as critical. This affects an unknown part of the file index.php. The manipulation of the argument username with the input ' AND (SELECT 4955 FROM (SELECT(SLEEP(5)))RSzF) AND 'htiy'='htiy leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205665 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2678	A vulnerability was found in SourceCodester Alphaware Simple E-Commerce System. It has been declared as critical. This vulnerability affects unknown code of the file admin_feature.php of the component Background Management Page. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-205666 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-2679	A vulnerability was found in SourceCodester Interview Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /viewReport.php. The manipulation of the argument id with the input (UPDATEXML(9729,CONCAT(0x2e,0x716b707071,(SELECT (ELT(9729=9729,1))),0x7162766a71),7319)) leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205667.	6.3	More Details
CVE-2022-2680	A vulnerability classified as critical has been found in SourceCodester Church Management System 1.0. Affected is an unknown function of the file /login.php. The manipulation of the argument username with the input ' OR (SELECT 7064 FROM(SELECT COUNT(*),CONCAT(0x71627a7671,(SELECT (ELT(7064=7064,1))),0x716b707871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- jURL leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-205668.	6.3	More Details
CVE-2022-2643	A vulnerability has been found in SourceCodester Online Admission System and classified as critical. This vulnerability affects unknown code of the component POST Parameter Handler. The manipulation of the argument shift leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this entry is VDB-205564.	6.3	More Details
CVE-2022-2648	A vulnerability was found in SourceCodester Multi Language Hotel Management Software. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument room_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205595.	6.3	More Details
CVE-2022-33201	Cross-Site Request Forgery (CSRF) vulnerability in MailerLite – Signup forms (official) plugin <= 1.5.7 at WordPress allows an attacker to change the API key.	6.3	More Details
CVE-2022-2656	A vulnerability classified as critical has been found in SourceCodester Multi Language Hotel Management Software. Affected is an unknown function. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-205596.	6.3	More Details
CVE-2022-2715	A vulnerability has been found in SourceCodester Employee Management System and classified as critical. This vulnerability affects unknown code of the file eloginwel.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-205834 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-2667	A vulnerability was found in SourceCodester Loan Management System and classified as critical. This issue affects some unknown processing of the file delete_lplan.php. The manipulation of the argument lplan_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205619.	6.3	More Details
CVE-2022-2687	A vulnerability, which was classified as critical, was found in SourceCodester Gym Management System. Affected is an unknown function. The manipulation of the argument user_pass leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-205734 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-2688	A vulnerability was found in SourceCodester Expense Management System. It has been rated as critical. This issue affects the function fetch_report_credit of the file report.php of the component POST Parameter Handler. The manipulation of the argument from/to leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-205811.	6.3	More Details
CVE-2022-2671	A vulnerability was found in SourceCodester Garage Management System and classified as critical. This issue affects some unknown processing of the file removeUser.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205655.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33732	Improper access control vulnerability in Samsung Dex for PC prior to SMR Aug-2022 Release 1 allows local attackers to scan and connect to PC by unprotected binder call.	6.2	More Details
CVE-2022-33733	Sensitive information exposure in onCharacteristicRead in Charm by Samsung prior to version 1.2.3 allows attacker to get bluetooth connection information without permission.	6.2	More Details
CVE-2022-33734	Sensitive information exposure in onCharacteristicChanged in Charm by Samsung prior to version 1.2.3 allows attacker to get bluetooth connection information without permission.	6.2	More Details
CVE-2022-33718	An improper access control vulnerability in Wi-Fi Service prior to SMR AUG-2022 Release 1 allows untrusted applications to manipulate the list of apps that can use mobile data.	6.2	More Details
CVE-2022-36829	PendingIntent hijacking vulnerability in releaseAlarm in Charm by Samsung prior to version 1.2.3 allows local attackers to access files without permission via implicit intent.	6.2	More Details
CVE-2022-2417	Insufficient validation in GitLab CE/EE affecting all versions from 12.10 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 allows an authenticated and authorised user to import a project that includes branch names which are 40 hexadecimal characters, which could be abused in supply chain attacks where a victim pinned to a specific Git commit of the project.	6.2	More Details
CVE-2022-36830	PendingIntent hijacking vulnerability in cancelAlarmManager in Charm by Samsung prior to version 1.2.3 allows local attackers to access files without permission via implicit intent.	6.2	More Details
CVE-2022-36831	Path traversal vulnerability in UriFileUtils of Samsung Notes prior to version 4.3.14.39 allows attacker to access some file as Samsung Notes permission.	6.2	More Details
CVE-2022-36836	Unprotected provider vulnerability in Charm by Samsung prior to version 1.2.3 allows attackers to read connection state without permission.	6.2	More Details
CVE-2022-36837	Intent redirection vulnerability using implicit intent in Samsung email prior to version 6.1.70.20 allows attacker to get sensitive information.	6.2	More Details
CVE-2022-33714	Improper access control vulnerability in SemWifiApBroadcastReceiver prior to SMR Aug-2022 Release 1 allows attacker to reset a setting value related to mobile hotspot.	6.2	More Details
CVE-2022-35776	Azure Site Recovery Denial of Service Vulnerability	6.2	More Details
CVE-2022-2731	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.1.	6.1	More Details
CVE-2022-2733	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.1.	6.1	More Details
CVE-2022-27166	A carefully crafted request on XHRHtml2Markup.jsp could trigger an XSS vulnerability on Apache JSPWiki up to and including 2.11.2, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim.	6.1	More Details
CVE-2022-37431	A Reflected Cross-site scripting (XSS) issue was discovered in dotCMS Core through 22.06. This occurs in the admin portal when the configuration has XSS_PROTECTION_ENABLED=false. NOTE: the vendor disputes this because the current product behavior, in effect, has XSS_PROTECTION_ENABLED=true in all configurations	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28732	A carefully crafted request on WeblogPlugin could trigger an XSS vulnerability on Apache JSPWiki, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.11.3 or later.	6.1	More Details
CVE-2022-28730	A carefully crafted request on AJAXPreview.jsp could trigger an XSS vulnerability on Apache JSPWiki, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. This vulnerability leverages CVE-2021-40369, where the Denounce plugin dangerously renders user-supplied URLs. Upon re-testing CVE-2021-40369, it appears that the patch was incomplete as it was still possible to insert malicious input via the Denounce plugin. Apache JSPWiki users should upgrade to 2.11.3 or later.	6.1	More Details
CVE-2022-36266	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists a stored XSS vulnerability. As the binary file /home/www/cgi-bin/login.cgi does not check if the user is authenticated, a malicious actor can craft a specific request on the login.cgi endpoint that contains a base32 encoded XSS payload that will be accepted and stored. A successful attack will results in the injection of malicious scripts into the user settings page.	6.1	More Details
CVE-2022-35493	A Cross-site scripting (XSS) vulnerability in json search parse and the json response in wrteam.in, eShop - Multipurpose Ecommerce Store Website version 3.0.4 allows remote attackers to inject arbitrary web script or HTML via the get_products?search parameter.	6.1	More Details
CVE-2022-35797	Windows Hello Security Feature Bypass Vulnerability	6.1	More Details
CVE-2022-31663	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window.	6.1	More Details
CVE-2022-2386	The Crowdsignal Dashboard WordPress plugin before 3.0.8 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-2652	Depending on the way the format strings in the card label are crafted it's possible to leak kernel stack memory. There is also the possibility for DoS due to the v4l2loopback kernel module crashing when providing the card label on request (reproduce e.g. with many %s modifiers in a row).	6.0	More Details
CVE-2022-34709	Windows Defender Credential Guard Security Feature Bypass Vulnerability	6.0	More Details
CVE-2022-35926	Contiki-NG is an open-source, cross-platform operating system for IoT devices. Because of insufficient validation of IPv6 neighbor discovery options in Contiki-NG, attackers can send neighbor solicitation packets that trigger an out-of-bounds read. The problem exists in the module os/net/ipv6/uip-nd6.c, where memory read operations from the main packet buffer, <code>uip_buf</code>, are not checked if they go out of bounds. In particular, this problem can occur when attempting to read the 2-byte option header and the Source Link-Layer Address Option (SLLAO). This attack requires ipv6 be enabled for the network. The problem has been patched in the develop branch of Contiki-NG. The upcoming 4.8 release of Contiki-NG will include the patch.Users unable to upgrade may apply the patch in Contiki-NG PR #1654.	5.9	More Details
CVE-2022-2501	An improper access control issue in GitLab EE affecting all versions from 12.0 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 allows an attacker to bypass IP allow-listing and download artifacts. This attack only bypasses IP allow-listing, proper permissions are still required.	5.9	More Details
CVE-2022-34716	.NET Spoofing Vulnerability	5.9	More Details
CVE-2022-33729	Improper restriction of broadcasting Intent in ConfirmConnectActivity of?NFC prior to SMR Aug-2022 Release 1 leaks MAC address of the connected Bluetooth device.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34844	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.9	More Details
CVE-2022-37450	Go Ethereum (aka geth) through 1.10.21 allows attackers to increase rewards by mining blocks in certain situations, and using a manipulation of time-difference values to achieve replacement of main-chain blocks, aka Riskless Uncle Making (RUM), as exploited in the wild in 2020 through 2022.	5.9	More Details
CVE-2022-36839	SQL injection vulnerability via IAPService in Samsung Checkout prior to version 5.0.53.1 allows attackers to access IAP information.	5.9	More Details
CVE-2022-31175	CKEditor 5 is a JavaScript rich text editor. A cross-site scripting vulnerability has been discovered affecting three optional CKEditor 5's packages in versions prior to 35.0.1. The vulnerability allowed to trigger a JavaScript code after fulfilling special conditions. The affected packages are `@ckeditor/ckeditor5-markdown-gfm`, `@ckeditor/ckeditor5-html-support`, and `@ckeditor/ckeditor5-html-embed`. The specific conditions are 1) Using one of the affected packages. In case of `ckeditor5-html-support` and `ckeditor5-html-embed`, additionally, it was required to use a configuration that allows unsafe markup inside the editor. 2) Destroying the editor instance and 3) Initializing the editor on an element and using an element other than `<textarea>` as a base. The root cause of the issue was a mechanism responsible for updating the source element with the markup coming from the CKEditor 5 data pipeline after destroying the editor. This vulnerability might affect a small percent of integrators that depend on dynamic editor initialization/destroy and use Markdown, General HTML Support or HTML embed features. The problem has been recognized and patched. The fix is available in version 35.0.1. There are no known workarounds for this issue.	5.8	More Details
CVE-2021-28511	This advisory documents the impact of an internally found vulnerability in Arista EOS for security ACL bypass. The impact of this vulnerability is that the security ACL drop rule might be bypassed if a NAT ACL rule filter with permit action matches the packet flow. This could allow a host with an IP address in a range that matches the range allowed by a NAT ACL and a range denied by a Security ACL to be forwarded incorrectly as it should have been denied by the Security ACL. This can enable an ACL bypass.	5.8	More Details
CVE-2022-34710	Windows Defender Credential Guard Information Disclosure Vulnerability	5.5	More Details
CVE-2022-2708	A vulnerability, which was classified as critical, was found in SourceCodester Gym Management System. This affects an unknown part of the file login.php. The manipulation of the argument user_login with the input 123@xx.com' OR (SELECT 9084 FROM(SELECT COUNT(*),CONCAT(0x7178767871,(SELECT (ELT(9084=9084,1))),0x71767a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- dPvW leads to sql injection. Access to the local network is required for this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-205833 was assigned to this vulnerability.	5.5	More Details
CVE-2022-34712	Windows Defender Credential Guard Information Disclosure Vulnerability	5.5	More Details
CVE-2022-2644	A vulnerability was found in SourceCodester Online Admission System and classified as critical. This issue affects some unknown processing of the component GET Parameter Handler. The manipulation of the argument eid leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-205565 was assigned to this vulnerability.	5.5	More Details
CVE-2022-34708	Windows Kernel Information Disclosure Vulnerability	5.5	More Details
CVE-2022-31618	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can dereference a null pointer, which may lead to denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30197	Windows Kernel Information Disclosure Vulnerability	5.5	More Details
CVE-2022-34686	Azure RTOS GUIX Studio Information Disclosure Vulnerability	5.5	More Details
CVE-2021-27798	A vulnerability in Brocade Fabric OS versions v7.4.1b and v7.3.1d could allow local users to conduct privileged directory transversal. Brocade Fabric OS versions v7.4.1.x and v7.3.x have reached end of life. Brocade Fabric OS Users should upgrade to supported versions as described in the Product End-of-Life Publish report	5.5	More Details
CVE-2022-34685	Azure RTOS GUIX Studio Information Disclosure Vulnerability	5.5	More Details
CVE-2022-27621	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology USB Copy before 2.2.0-1086 allows remote authenticated users to read or write arbitrary files via unspecified vectors.	5.5	More Details
CVE-2022-2734	Improper Restriction of Rendered UI Layers or Frames in GitHub repository openemr/openemr prior to 7.0.0.1.	5.4	More Details
CVE-2022-2391	The Inspiro PRO WordPress plugin does not sanitize the portfolio slider description, allowing users with privileges as low as Contributor to inject JavaScript into the description.	5.4	More Details
CVE-2022-27484	A unverified password change in Fortinet FortiADC version 6.2.0 through 6.2.3, 6.1.x, 6.0.x, 5.x.x allows an authenticated attacker to bypass the Old Password check in the password change form via a crafted HTTP request.	5.4	More Details
CVE-2022-33947	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, a vulnerability exists in undisclosed pages of the BIG-IP DNS Traffic Management User Interface (TMUI) that allows an authenticated attacker with at least operator role privileges to cause the Tomcat process to restart and perform unauthorized DNS requests and operations through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.4	More Details
CVE-2016-3098	Cross-site request forgery (CSRF) vulnerability in administrate 0.1.4 and earlier allows remote attackers to hijack the user's OAuth autorization code.	5.4	More Details
CVE-2020-1691	In Moodle 3.8, messages required extra sanitizing before updating the conversation overview, to prevent the risk of stored cross-site scripting.	5.4	More Details
CVE-2022-2371	The YaySMTP WordPress plugin before 2.2.1 does not have proper authorisation when saving its settings, allowing users with a role as low as subscriber to change them, and use that to conduct Stored Cross-Site Scripting attack due to the lack of escaping in them as well.	5.4	More Details
CVE-2022-36197	BigTree CMS 4.4.16 was discovered to contain an arbitrary file upload vulnerability which allows attackers to execute arbitrary code via a crafted PDF file.	5.4	More Details
CVE-2022-2729	Cross-site Scripting (XSS) - DOM in GitHub repository openemr/openemr prior to 7.0.0.1.	5.4	More Details
CVE-2021-36861	Cross-Site Request Forgery (CSRF) vulnerability in Rich Reviews by Starfish plugin <= 1.9.14 at WordPress allows an attacker to delete reviews.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27551	HCL Launch could allow an authenticated user to obtain sensitive information in some instances due to improper security checking.	5.3	More Details
CVE-2022-2539	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.6 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1, allowed a project member to filter issues by contact and organization.	5.3	More Details
CVE-2022-34692	Microsoft Exchange Server Information Disclosure Vulnerability	5.3	More Details
CVE-2022-2531	An issue has been discovered in GitLab EE affecting all versions starting from 12.5 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab was not performing correct authentication on Grafana API under specific conditions allowing unauthenticated users to perform queries through a path traversal vulnerability.	5.3	More Details
CVE-2022-33715	Improper access control and path traversal vulnerability in LauncherProvider prior to SMR Aug-2022 Release 1 allow local attacker to access files of One UI.	5.3	More Details
CVE-2022-33731	Improper access control vulnerability in DesktopSystemUI prior to SMR Aug-2022 Release 1 allows attackers to enable and disable arbitrary components.	5.1	More Details
CVE-2022-27617	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology Calendar before 2.3.4-0631 allows remote authenticated users to download arbitrary files via unspecified vectors.	5.0	More Details
CVE-2022-25649	Multiple Improper Access Control vulnerabilities in StoreApps Affiliate For WooCommerce premium plugin <= 4.7.0 at WordPress.	5.0	More Details
CVE-2022-35774	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-35812	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-2456	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for malicious group or project maintainers to change their corresponding group or project visibility by crafting a malicious POST request.	4.9	More Details
CVE-2022-35787	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-35800	Azure Site Recovery Elevation of Privilege Vulnerability	4.9	More Details
CVE-2022-2046	The Directorist WordPress plugin before 7.2.3 allows administrators to download other plugins from the same vendor directly to the site, but does not check the URL domain it gets the zip files from. This could allow administrators to run code on the server, which is a problem in multisite configurations.	4.9	More Details
CVE-2022-35162	Complete Online Job Search System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the CATEGORY parameter at /category/controller.php?action=edit.	4.8	More Details
CVE-2022-33727	A vulnerable code in onCreate of SecDevicePickerDialog prior to SMR Aug-2022 Release 1, allows attackers to trick the user to select an unwanted bluetooth device via tapjacking/overlay attack.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33723	A vulnerable code in onCreate of BluetoothScanDialog prior to SMR Aug-2022 Release 1, allows attackers to trick the user to select an unwanted bluetooth device via tapjacking/overlay attack.	4.8	More Details
CVE-2022-35163	Complete Online Job Search System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the U_NAME parameter at /category/controller.php?action=edit.	4.8	More Details
CVE-2022-2426	The Thinkific Uploader WordPress plugin through 1.0.0 does not sanitise and escape its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks against other administrators.	4.8	More Details
CVE-2022-34865	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.8	More Details
CVE-2022-35144	Renato v0.17.0 was discovered to contain a cross-site scripting (XSS) vulnerability.	4.8	More Details
CVE-2022-2411	The Auto More Tag WordPress plugin through 4.0.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-2372	The YaySMTP WordPress plugin before 2.2.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-2395	The weForms WordPress plugin before 1.6.14 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-2398	The WordPress Comments Fields WordPress plugin before 4.1 does not escape Field Error Message, which could allow high-privileged users to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-2409	The Rough Chart WordPress plugin through 1.0.0 does not properly escape chart data label, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-2410	The mTouch Quiz WordPress plugin through 3.1.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-21979	Microsoft Exchange Server Information Disclosure Vulnerability	4.8	More Details
CVE-2022-2412	The Better Tag Cloud WordPress plugin through 0.99.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-2423	The DW Promobar WordPress plugin through 1.0.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-2424	The Google Maps Anywhere WordPress plugin through 1.2.6.3 does not sanitise and escape any of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-2425	The WP DS Blog Map WordPress plugin through 3.1.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34704	Windows Defender Credential Guard Information Disclosure Vulnerability	4.7	More Details
CVE-2022-2700	A vulnerability classified as critical has been found in SourceCodester Gym Management System. This affects an unknown part of the component GET Parameter Handler. The manipulation of the argument day leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205821 was assigned to this vulnerability.	4.7	More Details
CVE-2022-30574	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, TIBCO eFTL - Enterprise Edition, and TIBCO eFTL - Enterprise Edition contains a difficult to exploit vulnerability that allows a low privileged attacker with local access to obtain user credentials to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, TIBCO FTL - Enterprise Edition: version 6.8.0, TIBCO eFTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO eFTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO eFTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO eFTL - Enterprise Edition: version 6.8.0.	4.6	More Details
CVE-2022-36840	DLL hijacking vulnerability in Samsung Update Setup prior to version 2.2.9.50 allows attackers to execute arbitrary code.	4.5	More Details
CVE-2022-35783	Azure Site Recovery Elevation of Privilege Vulnerability	4.4	More Details
CVE-2022-35821	Azure Sphere Information Disclosure Vulnerability	4.4	More Details
CVE-2022-33721	A vulnerability using PendingIntent in DeX for PC prior to SMR Aug-2022 Release 1 allows attackers to access files with system privilege.	4.4	More Details
CVE-2022-33717	A missing input validation before memory read in SEM TA prior to SMR Aug-2022 Release 1 allows local attackers to read out of bound memory.	4.4	More Details
CVE-2022-2500	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1. A stored XSS flaw in job error messages allows attackers to perform arbitrary actions on behalf of victims at client side.	4.4	More Details
CVE-2022-2303	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for group members to bypass 2FA enforcement enabled at the group level by using Resource Owner Password Credentials grant to obtain an access token without using 2FA.	4.3	More Details
CVE-2022-28880	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered remotely by an attacker.	4.3	More Details
CVE-2022-23442	An improper access control vulnerability [CWE-284] in FortiOS versions 6.2.0 through 6.2.11, 6.4.0 through 6.4.8 and 7.0.0 through 7.0.5 may allow an authenticated attacker with a restricted user profile to gather the checksum information about the other VDOMs via CLI commands.	4.3	More Details
CVE-2022-2095	An improper access control check in GitLab CE/EE affecting all versions starting from 13.7 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1 allows a malicious authenticated user to view a public project's Deploy Key's public fingerprint and name when that key has write permission. Note that GitLab never asks for nor stores the private key.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1754	In Moodle before 3.8.2, 3.7.5, 3.6.9 and 3.5.11, users viewing the grade history report without the 'access all groups' capability were not restricted to viewing grades of users within their own groups.	4.3	More Details
CVE-2022-34851	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.3	More Details
CVE-2022-36800	Affected versions of Atlassian Jira Service Management Server and Data Center allow remote attackers without the "Browse Users" permission to view groups via an Information Disclosure vulnerability in the browsegroups.action endpoint. The affected versions are before version 4.22.2.	4.3	More Details
CVE-2022-2704	A vulnerability was found in SourceCodester Simple E-Learning System. It has been declared as problematic. This vulnerability affects unknown code of the file downloadFiles.php. The manipulation of the argument download leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-205828.	4.3	More Details
CVE-2022-37396	In JetBrains Rider before 2022.2 Trust and Open Project dialog could be bypassed, leading to local code execution	4.1	More Details
CVE-2022-33725	A vulnerability using PendingIntent in Knox VPN prior to SMR Aug-2022 Release 1 allows attackers to access content providers with system privilege.	4.0	More Details
CVE-2022-36838	Implicit Intent hijacking vulnerability in Galaxy Wearable prior to version 2.2.50 allows attacker to get sensitive information.	4.0	More Details
CVE-2021-46679	A XSS vulnerability exist in Pandora FMS version 756 and below, that allows an attacker to perform javascript code executions via service elements.	4.0	More Details
CVE-2021-46676	A XSS vulnerability exist in Pandora FMS version 756 and below, that allows an attacker to perform javascript code executions via the transactional maps name field.	4.0	More Details
CVE-2022-36832	Improper access control vulnerability in WebApp in Cameralyzer prior to versions 3.2.22, 3.3.22, 3.4.22 and 3.5.51 allows attackers to access external storage as Cameralyzer privilege.	4.0	More Details
CVE-2021-46677	A XSS vulnerability exist in Pandora FMS version 756 and below, that allows an attacker to perform javascript code executions via the event filter name field.	4.0	More Details
CVE-2021-46678	A XSS vulnerability exist in Pandora FMS version 756 and below, that allows an attacker to perform javascript code executions via the service name field.	4.0	More Details
CVE-2022-33728	Exposure of sensitive information in Bluetooth prior to SMR Aug-2022 Release 1 allows local attackers to access connected BT macAddress via Settings.Gloabal.	4.0	More Details
CVE-2021-46680	A XSS vulnerability exist in Pandora FMS version 756 and below, that allows an attacker to perform javascript code executions via the module form name field.	4.0	More Details
CVE-2022-29071	This advisory documents an internally found vulnerability in the on premises deployment model of Arista CloudVision Portal (CVP) where under a certain set of conditions, user passwords can be leaked in the Audit and System logs. The impact of this vulnerability is that the CVP user login passwords might be leaked to other authenticated users.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46681	A XSS vulnerability exist in Pandora FMS version 756 and below, that allows an attacker to perform javascript code executions via module massive operation name field.	4.0	More Details
CVE-2022-33722	Implicit Intent hijacking vulnerability in Smart View prior to SMR Aug-2022 Release 1 allows attacker to access connected device MAC address.	4.0	More Details
CVE-2022-33968	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	3.7	More Details
CVE-2022-2689	A vulnerability classified as problematic has been found in SourceCodester Wedding Hall Booking System. Affected is an unknown function of the file /whbs/?page=contact_us of the component Contact Page. The manipulation of the argument Message 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. The identifier of this vulnerability is VDB-205812.	3.5	More Details
CVE-2022-2686	A vulnerability, which was classified as problematic, was found in oretnom23 Fast Food Ordering System. This affects an unknown part of the component Menu List Page. The manipulation of the argument Description 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. The identifier VDB-205725 was assigned to this vulnerability.	3.5	More Details
CVE-2022-2499	An issue has been discovered in GitLab EE affecting all versions starting from 13.10 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab's Jira integration has an insecure direct object reference vulnerability that may be exploited by an attacker to leak Jira issues.	3.5	More Details
CVE-2022-2690	A vulnerability classified as problematic was found in SourceCodester Wedding Hall Booking System. Affected by this vulnerability is an unknown functionality of the file /whbs/?page=my_bookings of the component Booking Form. The manipulation of the argument Remarks leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205813 was assigned to this vulnerability.	3.5	More Details
CVE-2022-2645	A vulnerability has been found in SourceCodester Garage Management System and classified as problematic. Affected by this vulnerability is an unknown functionality of the file edituser.php. The manipulation of the argument id with the input 1\"><ScRiPt>alert(1)</sCrIpT> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205573 was assigned to this vulnerability.	3.5	More Details
CVE-2022-2691	A vulnerability, which was classified as problematic, has been found in SourceCodester Wedding Hall Booking System. Affected by this issue is some unknown functionality of the file /whbs/?page=manage_account of the component Profile Page. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-205814 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-2692	A vulnerability, which was classified as problematic, was found in SourceCodester Wedding Hall Booking System. This affects an unknown part of the file /whbs/admin/?page=user of the component Staff User Profile. The manipulation of the argument First Name/Last Name 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. The associated identifier of this vulnerability is VDB-205815.	3.5	More Details
CVE-2022-2646	A vulnerability, which was classified as problematic, was found in SourceCodester Online Admission System. Affected is an unknown function of the file index.php. The manipulation of the argument eid with the input 8</h3><script>alert(1)</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. The identifier of this vulnerability is VDB-205572.	3.5	More Details
CVE-2022-2701	A vulnerability classified as problematic was found in SourceCodester Simple E-Learning System. This vulnerability affects unknown code of the file /claire_blake. The manipulation of the argument Bio leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-205822 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2685	A vulnerability was found in SourceCodester Interview Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /addQuestion.php. The manipulation of the argument question with the input <script>alert(1)</script> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205673 was assigned to this vulnerability.	3.5	More Details
CVE-2022-2307	A lack of cascading deletes in GitLab CE/EE affecting all versions starting from 13.0 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1 allows a malicious Group Owner to retain a usable Group Access Token even after the Group is deleted, though the APIs usable by that token are limited.	3.5	More Details
CVE-2022-2725	A vulnerability was found in SourceCodester Company Website CMS. It has been rated as problematic. Affected by this issue is some unknown functionality of the file add-blog.php. The manipulation leads to cross site scripting. The attack may be launched remotely. VDB-205838 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-2684	A vulnerability has been found in SourceCodester Apartment Visitor Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /manage-apartment.php. The manipulation of the argument Apartment Number with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-205672.	3.5	More Details
CVE-2022-2681	A vulnerability classified as problematic was found in SourceCodester Online Student Admission System. Affected by this vulnerability is an unknown functionality of the file edit-profile.php of the component Student User Page. The manipulation 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. The identifier VDB-205669 was assigned to this vulnerability.	3.5	More Details
CVE-2022-2682	A vulnerability, which was classified as problematic, has been found in SourceCodester Alphaware Simple E-Commerce System. Affected by this issue is some unknown functionality of the file stockin.php. The manipulation of the argument id 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. VDB-205670 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-2683	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Food Ordering System 1.0. This affects an unknown part of the file /login.php. The manipulation of the argument email/password with the input "><ScRiPt>alert(1)</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. The associated identifier of this vulnerability is VDB-205671.	3.5	More Details
CVE-2022-33724	Exposure of Sensitive Information in Samsung Dialer application?prior to SMR Aug-2022 Release 1 allows local attackers to access ICCID via log.	3.3	More Details
CVE-2022-37394	An issue was discovered in OpenStack Nova before 23.2.2, 24.x before 24.1.2, and 25.x before 25.0.2. By creating a neutron port with the direct vnic_type, creating an instance bound to that port, and then changing the vnic_type of the bound port to macvtap, an authenticated user may cause the compute service to fail to restart, resulting in a possible denial of service. Only Nova deployments configured with SR-IOV are affected.	3.3	More Details
CVE-2022-33726	Unprotected dynamic receiver in Samsung Galaxy Friends prior to SMR Aug-2022 Release 1 allows attacker to launch activity.	3.3	More Details
CVE-2022-36834	Exposure of Sensitive Information vulnerability in Game Launcher prior to version 6.0.07 allows local attacker to access app data with user interaction.	3.3	More Details
CVE-2022-36835	Implicit Intent hijacking vulnerability in Samsung Internet Browser prior to version 17.0.7.34 allows attackers to access arbitrary files.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31119	Nextcloud Mail is an email application for the nextcloud personal cloud product. Affected versions of Nextcloud mail would log user passwords to disk in the event of a misconfiguration. Should an attacker gain access to the logs complete access to affected accounts would be obtainable. It is recommended that the Nextcloud Mail is upgraded to 1.12.1. Operators should inspect their logs and remove passwords which have been logged. There are no workarounds to prevent logging in the event of a misconfiguration.	3.1	More Details
CVE-2022-2459	An issue has been discovered in GitLab EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for email invited members to join a project even after the Group Owner has enabled the setting to prevent members from being added to projects in a group, if the invite was sent before the setting was enabled.	2.7	More Details
CVE-2022-33720	Improper authentication vulnerability in AppLock prior to SMR Aug-2022 Release 1 allows physical attacker to access Chrome locked by AppLock via new tap shortcut.	2.4	More Details
CVE-2022-33716	An absence of variable initialization in ICCC TA prior to SMR Aug-2022 Release 1 allows local attacker to read uninitialized memory.	2.3	More Details
CVE-2022-2534	An issue has been discovered in GitLab CE/EE affecting all versions starting from 9.3 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab was returning contributor emails due to improper data handling in the Datadog integration.	2.2	More Details
CVE-2022-31120	Nextcloud server is an open source personal cloud solution. The audit log is used to get a full trail of the actions which has been incompletely populated. In affected versions federated share events were not properly logged which would allow brute force attacks to go unnoticed. This behavior exacerbates the impact of CVE-2022-31118. It is recommended that the Nextcloud Server is upgraded to 22.2.7, 23.0.4 or 24.0.0. There are no workarounds available.	2.1	More Details
CVE-2022-34943	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-2018-1076	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2019-10204	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-2017-15106	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 2017. Notes: none	N/A	More Details
CVE-2017-12152	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 2017. Notes: none	N/A	More Details
CVE-2021-43178	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 2021. Notes: none	N/A	More Details
CVE-2017-15109	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 2017. Notes: none	N/A	More Details
CVE-2017-15122	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 2017. Notes: none	N/A	More Details
CVE-2017-2588	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 2017. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-2593	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 2017. Notes: none	N/A	More Details
CVE-2017-2597	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 2017. Notes: none	N/A	More Details
CVE-2017-2631	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 2017. Notes: none	N/A	More Details
CVE-2017-7527	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 2017. Notes: none	N/A	More Details
CVE-2021-43179	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 2021. Notes: none	N/A	More Details
CVE-2017-2657	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 2017. Notes: none	N/A	More Details