SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 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-2022-30547	A directory traversal vulnerability exists in the unzipDirectory functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability.	9.9	More Details
CVE-2022-36220	Kiosk breakout (without quit password) in Safe Exam Browser (Windows) <3.4.0, which allows an attacker to achieve code execution via the browsers' print dialog.	9.8	More Details
CVE-2022-34149	Authentication Bypass vulnerability in miniOrange WP OAuth Server plugin <= 3.0.4 at WordPress.	9.8	More Details
CVE-2022-36190	GPAC mp4box 2.1-DEV-revUNKNOWN-master has a use-after-free vulnerability in function gf_isom_dovi_config_get. This vulnerability was fixed in commit fef6242.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34615	Mealie 1.0.0beta3 employs weak password requirements which allows attackers to potentially gain unauthorized access to the application via brute-force attacks.	9.8	More Details
CVE-2022-35201	Tenda-AC18 V15.03.05.05 was discovered to contain a remote command execution (RCE) vulnerability.	9.8	More Details
CVE-2022-36605	Yimioa v6.1 was discovered to contain a SQL injection vulnerability via the orderbyGET parameter.	9.8	More Details
CVE-2022-36606	Ywoa before v6.1 was discovered to contain a SQL injection vulnerability via /oa/setup/checkPool?database.	9.8	More Details
CVE-2022-36578	jizhicms v2.3.1 has SQL injection in the background.	9.8	More Details
CVE-2022-37175	Tenda ac15 firmware V15.03.05.18 httpd server has stack buffer overflow in /goform/formWifiBasicSet.	9.8	More Details
CVE-2022-36030	Project-nexus is a general-purpose blog website framework. Affected versions are subject to SQL injection due to a lack of sensitization of user input. This issue has not yet been patched. Users are advised to restrict user input and to upgrade when a new release becomes available.	9.8	More Details
CVE-2022-34916	Apache Flume versions 1.4.0 through 1.10.0 are vulnerable to a remote code execution (RCE) attack when a configuration uses a JMS Source with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI to allow only the use of the java protocol or no protocol.	9.8	More Details
CVE-2022-36198	Multiple SQL injections detected in Bus Pass Management System 1.0 via buspassms/admin/view-enquiry.php, buspassms/admin/pass-bwdates-reports-details.php, buspassms/admin/changeimage.php, buspassms/admin/search-pass.php, buspassms/admin/edit-category-detail.php, and buspassms/admin/edit-pass-detail.php	9.8	More Details
CVE-2022-2927	Weak Password Requirements in GitHub repository notrinos/notrinoserp prior to 0.7.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27836	A flaw was found in cluster-ingress-operator. A change to how the router-default service allows only certain IP source ranges could allow an attacker to access resources that would otherwise be restricted to specified IP ranges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability..	9.8	More Details
CVE-2021-3586	A flaw was found in servicemesh-operator. The NetworkPolicy resources installed for Maistra do not properly specify which ports may be accessed, allowing access to all ports on these resources from any pod. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	9.8	More Details
CVE-2022-34858	Authentication Bypass vulnerability in miniOrange OAuth 2.0 client for SSO plugin <= 1.11.3 at WordPress.	9.8	More Details
CVE-2022-35540	Hardcoded JWT Secret in AgileConfig <1.6.8 Server allows remote attackers to use the generated JWT token to gain administrator access.	9.8	More Details
CVE-2022-37134	D-link DIR-816 A2_v1.10CNB04.img is vulnerable to Buffer Overflow via /goform/form2Wan.cgi. When wantype is 3, l2tp_usrname will be decrypted by base64, and the result will be stored in v94, which does not check the size of l2tp_usrname, resulting in stack overflow.	9.8	More Details
CVE-2022-35150	Baijicms v4 was discovered to contain an arbitrary file upload vulnerability.	9.8	More Details
CVE-2022-35583	wkhtmlTOpdf 0.12.6 is vulnerable to SSRF which allows an attacker to get initial access into the target's system by injecting iframe tag with initial asset IP address on it's source. This allows the attacker to takeover the whole infrastructure by accessing their internal assets.	9.8	More Details
CVE-2022-38667	HTTP applications (servers) based on Crow through 1.0+4 may allow a Use-After-Free and code execution when HTTP pipelining is used. The HTTP parser supports HTTP pipelining, but the asynchronous Connection layer is unaware of HTTP pipelining. Specifically, the Connection layer is unaware that it has begun processing a later request before it has finished processing an earlier request.	9.8	More Details
CVE-2021-42232	TP-Link Archer A7 Archer A7(US)_V5_210519 is affected by a command injection vulnerability in /usr/bin/tddp. The vulnerability is caused by the program taking part of the received data packet as part of the command. This will cause an attacker to execute arbitrary commands on the router.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34919	The file upload wizard in Zengenti Contensis Classic before 15.2.1.79 does not correctly check that a user has authenticated. By uploading a crafted aspx file, it is possible to execute arbitrary commands.	9.8	More Details
CVE-2022-35733	Missing authentication for critical function vulnerability in UNIMO Technology digital video recorders (UDR-JA1004/JA1008/JA1016 firmware versions v1.0.20.13 and earlier, and UDR-JA1016 firmware versions v2.0.20.13 and earlier) allows a remote unauthenticated attacker to execute an arbitrary OS command by sending a specially crafted request to the affected device web interface.	9.8	More Details
CVE-2021-42627	The WAN configuration page "wan.htm" on D-Link DIR-615 devices with firmware 20.06 can be accessed directly without authentication which can lead to disclose the information about WAN settings and also leverage attacker to modify the data fields of page.	9.8	More Details
CVE-2022-37199	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /jfinal_cms/system/user/list.	9.8	More Details
CVE-2022-37223	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /jfinal_cms/system/role/list.	9.8	More Details
CVE-2022-37111	BlueCMS 1.6 has SQL injection in line 132 of admin/article.php	9.8	More Details
CVE-2022-37112	BlueCMS 1.6 has SQL injection in line 55 of admin/model.php	9.8	More Details
CVE-2022-37113	Bluecms 1.6 has SQL injection in line 132 of admin/area.php	9.8	More Details
CVE-2022-29805	A Java Deserialization vulnerability in the Fishbowl Server in Fishbowl Inventory before 2022.4.1 allows remote attackers to execute arbitrary code via a crafted XML payload.	9.8	More Details
CVE-2022-35115	IceWarp WebClient DC2 - Update 2 Build 9 (13.0.2.9) was discovered to contain a SQL injection vulnerability via the search parameter at /webmail/server/webmail.php.	9.8	More Details
CVE-2020-36599	lib/omniauth/failure_endpoint.rb in OmniAuth before 1.9.2 (and before 2.0) does not escape the message_key value.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35154	Shopro Mall System v1.3.8 was discovered to contain a SQL injection vulnerability via the value parameter.	9.8	More Details
CVE-2022-22455	IBM Security Verify Governance Identity Manager 10.0 virtual appliance component performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses. IBM X-Force ID: 224989.	9.8	More Details
CVE-2022-35121	Novel-Plus v3.6.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /service/impl/BookServiceImpl.java.	9.8	More Details
CVE-2022-35516	DedeCMS v5.7.93 - v5.7.96 was discovered to contain a remote code execution vulnerability in login.php.	9.8	More Details
CVE-2022-23747	In Sony Xperia series 1, 5, and Pro, an out of bound memory access can occur due to lack of validation of the number of frames being passed during music playback.	9.8	More Details
CVE-2022-2336	Softing Secure Integration Server, edgeConnector, and edgeAggregator software ships with the default administrator credentials as `admin` and password as `admin`. This allows Softing to log in to the server directly to perform administrative functions. Upon installation or upon first login, the application does not ask the user to change the `admin` password. There is no warning or prompt to ask the user to change the default password, and to change the password, many steps are required.	9.8	More Details
CVE-2022-35147	DoraCMS v2.18 and earlier allows attackers to bypass login authentication via a crafted HTTP request.	9.8	More Details
CVE-2022-35598	A SQL injection vulnerability in ConnectionFactoryDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via parameter username.	9.8	More Details
CVE-2022-35599	A SQL injection vulnerability in Stocks.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via parameter productcode.	9.8	More Details
CVE-2022-35601	A SQL injection vulnerability in SupplierDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via parameter searchTxt.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35602	A SQL injection vulnerability in UserDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via parameter user.	9.8	More Details
CVE-2022-35603	A SQL injection vulnerability in CustomerDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via parameter searchTxt.	9.8	More Details
CVE-2022-35605	A SQL injection vulnerability in UserDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via the parameters such as 'users', 'pass', etc.	9.8	More Details
CVE-2022-36947	Unsafe Parsing of a PNG tRNS chunk in FastStone Image Viewer through 7.5 results in a stack buffer overflow.	9.8	More Details
CVE-2022-35153	FusionPBX 5.0.1 was discovered to contain a command injection vulnerability via /fax/fax_send.php.	9.8	More Details
CVE-2022-35606	A SQL injection vulnerability in CustomerDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via the parameter 'customerCode.'	9.8	More Details
CVE-2022-35164	LibreDWG v0.12.4.4608 & commit f2dea29 was discovered to contain a heap use-after-free via bit_copy_chain.	9.8	More Details
CVE-2022-35175	Barangay Management System v1.0 was discovered to contain a SQL injection vulnerability via the hidden_id parameter at /blotter/blotter.php.	9.8	More Details
CVE-2022-30601	Insufficiently protected credentials for Intel(R) AMT and Intel(R) Standard Manageability may allow an unauthenticated user to potentially enable information disclosure and escalation of privilege via network access.	9.8	More Details
CVE-2022-36729	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the M_Id parameter at /librarian/del.php.	9.8	More Details
CVE-2022-36728	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the RollNo parameter at /staff/delstu.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36727	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the bookId parameter at /staff/delete.php.	9.8	More Details
CVE-2022-36725	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the M_Id parameter at /student/dele.php.	9.8	More Details
CVE-2022-36722	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the title parameter at /librarian/history.php.	9.8	More Details
CVE-2022-25899	Authentication bypass for the Open AMT Cloud Toolkit software maintained by Intel(R) before versions 2.0.2 and 2.2.2 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	9.8	More Details
CVE-2022-22730	Improper authentication in the Intel(R) Edge Insights for Industrial software before version 2.6.1 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	9.8	More Details
CVE-2022-37061	All FLIR AX8 thermal sensor cameras version up to and including 1.46.16 are vulnerable to Remote Command Injection. This can be exploited to inject and execute arbitrary shell commands as the root user through the id HTTP POST parameter in the res.php endpoint. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the root privileges.	9.8	More Details
CVE-2022-26842	A reflected cross-site scripting (xss) vulnerability exists in the charts tab selection functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.	9.6	More Details
CVE-2020-27794	A double free issue was discovered in radare2 in cmd_info.c:cmd_info(). Successful exploitation could lead to modification of unexpected memory locations and potentially causing a crash.	9.1	More Details
CVE-2022-22489	IBM MQ 8.0, (9.0, 9.1, 9.2 LTS), and (9.1 and 9.2 CD) are vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 226339.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35122	An access control issue in Ecowitt GW1100 Series Weather Stations <=GW1100B_v2.1.5 allows unauthenticated attackers to access sensitive information including device and local WiFi passwords.	9.1	More Details
CVE-2022-36261	An arbitrary file deletion vulnerability was discovered in taocms 3.0.2, that allows attacker to delete file in server when request url admin.php?action=file&ctrl=del&path=/../../../test.txt	9.1	More Details
CVE-2022-1399	An Argument Injection or Modification vulnerability in the "Change Secret" username field as used in the Discovery component of Device42 CMDB allows a local attacker to run arbitrary code on the appliance with root privileges. This issue affects: Device42 CMDB version 18.01.00 and prior versions.	9.1	More Details
CVE-2022-28712	A cross-site scripting (xss) vulnerability exists in the videoAddNew functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.	9.0	More Details
CVE-2022-35975	The GitOps Tools Extension for VSCode can make it easier to manage Flux objects. A specially crafted Flux object may allow for remote code execution in the machine running the extension, in the context of the user that is running VSCode. Users using the VSCode extension to manage clusters that are shared amongst other users are affected by this issue. The only safe mitigation is to update to the latest version of the extension.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-21139	Inadequate encryption strength for some Intel(R) PROSet/Wireless WiFi products may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2022-36224	XunRuiCMS V4.5.6 is vulnerable to Cross Site Request Forgery (CSRF).	8.8	More Details
CVE-2022-36225	EyouCMS V1.5.8-UTF8-SP1 is vulnerable to Cross Site Request Forgery (CSRF) via the background, column management function and add.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23764	The vulnerability causing from insufficient verification procedures for downloaded files during WebCube update. Remote attackers can bypass this verification logic to update both digitally signed and unauthorized files, enabling remote code execution.	8.8	More Details
CVE-2022-32282	An improper password check exists in the login functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. An attacker that owns a users' password hash will be able to use it to directly login into the account, leading to increased privileges.	8.8	More Details
CVE-2022-36579	Wellcms 2.2.0 is vulnerable to Cross Site Request Forgery (CSRF).	8.8	More Details
CVE-2022-32572	An os command injection vulnerability exists in the aVideoEncoder wget functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2022-34868	Authenticated Arbitrary Settings Update vulnerability in YooMoney ЮKassa для WooCommerce plugin <= 2.3.0 at WordPress.	8.8	More Details
CVE-2022-28751	The Zoom Client for Meetings for MacOS (Standard and for IT Admin) before version 5.11.3 contains a vulnerability in the package signature validation during the update process. A local low-privileged user could exploit this vulnerability to escalate their privileges to root.	8.8	More Details
CVE-2022-28752	Zoom Rooms for Conference Rooms for Windows versions before 5.11.0 are susceptible to a Local Privilege Escalation vulnerability. A local low-privileged malicious user could exploit this vulnerability to escalate their privileges to the SYSTEM user.	8.8	More Details
CVE-2022-33147	A sql injection vulnerability exists in the ObjectYPT functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to a SQL injection. An attacker can send an HTTP request to trigger this vulnerability.This vulnerability exists in the aVideoEncoder functionality which can be used to add new videos, allowing an attacker to inject SQL by manipulating the videoDownloadedLink or duration parameter.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33148	A sql injection vulnerability exists in the ObjectYPT functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to a SQL injection. An attacker can send an HTTP request to trigger this vulnerability.This vulnerability exists in the Live Schedules plugin, allowing an attacker to inject SQL by manipulating the title parameter.	8.8	More Details
CVE-2022-36170	MapGIS 10.5 Pro IGServer has hardcoded credentials in the front-end and can lead to escalation of privileges and arbitrary file deletion.	8.8	More Details
CVE-2022-36157	XXL-JOB all versions as of 11 July 2022 are vulnerable to Insecure Permissions resulting in the ability to execute admin function with low Privilege account.	8.8	More Details
CVE-2022-28757	The Zoom Client for Meetings for macOS (Standard and for IT Admin) starting with version 5.7.3 and before 5.11.6 contains a vulnerability in the auto update process. A local low-privileged user could exploit this vulnerability to escalate their privileges to root.	8.8	More Details
CVE-2022-33149	A sql injection vulnerability exists in the ObjectYPT functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to a SQL injection. An attacker can send an HTTP request to trigger this vulnerability.This vulnerability exists in the CloneSite plugin, allowing an attacker to inject SQL by manipulating the url parameter.	8.8	More Details
CVE-2022-34652	A sql injection vulnerability exists in the ObjectYPT functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to a SQL injection. An attacker can send an HTTP request to trigger this vulnerability.This vulnerability exists in the Live Schedules plugin, allowing an attacker to inject SQL by manipulating the description parameter.	8.8	More Details
CVE-2022-23182	Improper access control in the Intel(R) Data Center Manager software before version 4.1 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2022-30036	MA Lighting grandMA2 Light has a password of root for the root account. NOTE: The vendor's position is that the product was designed for isolated networks. Also, the successor product, grandMA3, is not affected by this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30605	A privilege escalation vulnerability exists in the session id functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to increased privileges. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2022-36577	An issue was discovered in jizhicms v2.3.1. There is a CSRF vulnerability that can add a admin.	8.8	More Details
CVE-2022-2921	Exposure of Private Personal Information to an Unauthorized Actor in GitHub repository notrinos/notrinoserp prior to v0.7. This results in privilege escalation to a system administrator account. An attacker can gain access to protected functionality such as create/update companies, install/update languages, install/activate extensions, install/activate themes and other permissive actions.	8.8	More Details
CVE-2022-35909	In Jellyfin before 10.8, the /users endpoint has incorrect access control for admin functionality.	8.8	More Details
CVE-2022-30534	An OS command injection vulnerability exists in the aVideoEncoder chunkfile functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2022-2557	The Team WordPress plugin before 4.1.2 contains a file which could allow any authenticated users to download arbitrary files from the server via a path traversal vector. Furthermore, the file will also be deleted after its content is returned to the user	8.8	More Details
CVE-2022-29468	A cross-site request forgery (CSRF) vulnerability exists in WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to increased privileges. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2022-2594	The Advanced Custom Fields WordPress plugin before 5.12.3, Advanced Custom Fields Pro WordPress plugin before 5.12.3 allows unauthenticated users to upload files allowed in a default WP configuration (so PHP is not possible) if there is a frontend form available. This vulnerability was introduced in the 5.0 rewrite and did not exist prior to that release.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3590	A flaw was found in Foreman project. A credential leak was identified which will expose Azure Compute Profile password through JSON of the API output. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.8	More Details
CVE-2022-35167	Printix Cloud Print Management v1.3.1149.0 for Windows was discovered to contain insecure permissions.	8.8	More Details
CVE-2022-36379	Cross-Site Request Forgery (CSRF) leading to plugin settings update in YooMoney ЮKassa для WooCommerce plugin <= 2.3.0 at WordPress.	8.8	More Details
CVE-2022-36171	MapGIS IGServer 10.5.6.11 is vulnerable to Arbitrary file deletion.	8.1	More Details
CVE-2021-26639	This vulnerability is caused by the lack of validation of input values for specific functions if WISA Smart Wing CMS. Remote attackers can use this vulnerability to leak all files in the server without logging in system.	8.1	More Details
CVE-2022-23459	Jsonxx or Json++ is a JSON parser, writer and reader written in C++. In affected versions of jsonxx use of the Value class may lead to memory corruption via a double free or via a use after free. The value class has a default assignment operator which may be used with pointer types which may point to alterable data where the pointer itself is not updated. This issue exists on the current commit of the jsonxx project. The project itself has been archived and updates are not expected. Users are advised to find a replacement.	8.1	More Details
CVE-2022-2625	A vulnerability was found in PostgreSQL. This attack requires permission to create non-temporary objects in at least one schema, the ability to lure or wait for an administrator to create or update an affected extension in that schema, and the ability to lure or wait for a victim to use the object targeted in CREATE OR REPLACE or CREATE IF NOT EXISTS. Given all three prerequisites, this flaw allows an attacker to run arbitrary code as the victim role, which may be a superuser.	8.0	More Details
CVE-2022-1410	OS Command Injection vulnerability in the db_optimize component of Device42 Asset Management Appliance allows an authenticated attacker to execute remote code on the device. This issue affects: Device42 CMDB version 18.01.00 and prior versions.	8.0	More Details
CVE-2022-26017	Improper access control in the Intel(R) DSA software for before version 22.2.14 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21225	Improper neutralization in the Intel(R) Data Center Manager software before version 4.1 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	8.0	More Details
CVE-2022-23765	This vulnerability occured by sending a malicious POST request to a specific page while logged in random user from some family of IPTIME NAS. Remote attackers can steal root privileges by changing the password of the root through a POST request.	8.0	More Details
CVE-2022-21812	Improper access control in the Intel(R) HAXM software before version 7.7.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-23223	Improper initialization for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi products may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-21229	Improper buffer restrictions for some Intel(R) NUC 9 Extreme Laptop Kit drivers before version 2.2.0.22 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-38171	Xpdf prior to version 4.04 contains an integer overflow in the JBIG2 decoder (JBIG2Stream::readTextRegionSeg() in JBIG2Stream.cc). Processing a specially crafted PDF file or JBIG2 image could lead to a crash or the execution of arbitrary code. This is similar to the vulnerability described by CVE-2021-30860 (Apple CoreGraphics).	7.8	More Details
CVE-2021-37409	Improper access control for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi products may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33847	Improper buffer restrictions in firmware for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products before version 22.120 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-37025	An improper privilege management vulnerability in McAfee Security Scan Plus (MSS+) before 4.1.262.1 could allow a local user to modify a configuration file and perform a LOLBin (Living off the land) attack. This could result in the user gaining elevated permissions and being able to execute arbitrary code due to lack of an integrity check of the configuration file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25972	An out-of-bounds write vulnerability exists in the gif2h5 functionality of HDF5 Group libhdf5 1.10.4. A specially-crafted GIF file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-2930	Unverified Password Change in GitHub repository octoprint/octoprint prior to 1.8.3.	7.8	More Details
CVE-2022-21181	Improper input validation for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi products may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-25942	An out-of-bounds read vulnerability exists in the gif2h5 functionality of HDF5 Group libhdf5 1.10.4. A specially-crafted GIF file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2021-33060	Out-of-bounds write in the BIOS firmware for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-25841	Uncontrolled search path elements in the Intel(R) Datacenter Group Event Android application, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-26061	A heap-based buffer overflow vulnerability exists in the gif2h5 functionality of HDF5 Group libhdf5 1.10.4. A specially-crafted GIF file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-21807	Uncontrolled search path elements in the Intel(R) VTune(TM) Profiler software before version 2022.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-21148	Improper access control in the Intel(R) Edge Insights for Industrial software before version 2.6.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-31676	VMware Tools (12.0.0, 11.x.y and 10.x.y) contains a local privilege escalation vulnerability. A malicious actor with local non-administrative access to the Guest OS can escalate privileges as a root user in the virtual machine.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27493	Improper initialization in the firmware for some Intel(R) NUC Laptop Kits before version BC0076 may allow a privileged user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2022-25966	Improper access control in the Intel(R) Edge Insights for Industrial software before version 2.6.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-2938	A flaw was found in the Linux kernel's implementation of Pressure Stall Information. While the feature is disabled by default, it could allow an attacker to crash the system or have other memory-corruption side effects.	7.8	More Details
CVE-2022-37459	Ampere Altra devices before 1.08g and Ampere Altra Max devices before 2.05a allow attackers to control the predictions for return addresses and potentially hijack code flow to execute arbitrary code via a side-channel attack, aka a "Retbleed" issue.	7.8	More Details
CVE-2022-2845	Improper Validation of Specified Quantity in Input in GitHub repository vim/vim prior to 9.0.0218.	7.8	More Details
CVE-2022-30262	The Emerson ControlWave 'Next Generation' RTUs through 2022-05-02 mishandle firmware integrity. They utilize the BSAP-IP protocol to transmit firmware updates. Firmware updates are supplied as CAB archive files containing a binary firmware image. In all cases, firmware images were found to have no authentication (in the form of firmware signing) and only relied on insecure checksums for regular integrity checks.	7.8	More Details
CVE-2022-31262	An exploitable local privilege escalation vulnerability exists in GOG Galaxy 2.0.46. Due to insufficient folder permissions, an attacker can hijack the %ProgramData%\GOG.com folder structure and change the GalaxyCommunication service executable to a malicious file, resulting in code execution as SYSTEM.	7.8	More Details
CVE-2022-2889	Use After Free in GitHub repository vim/vim prior to 9.0.0225.	7.8	More Details
CVE-2020-35511	A global buffer overflow was discovered in pngcheck function in pngcheck-2.4.0(5 patches applied) via a crafted png file.	7.8	More Details
CVE-2022-2849	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0220.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2946	Use After Free in GitHub repository vim/vim prior to 9.0.0246.	7.8	More Details
CVE-2022-2862	Use After Free in GitHub repository vim/vim prior to 9.0.0221.	7.8	More Details
CVE-2022-34488	Improper buffer restrictions in the firmware for some Intel(R) NUC Laptop Kits before version BC0076 may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-33209	Improper input validation in the firmware for some Intel(R) NUC Laptop Kits before version BC0076 may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-28858	Improper buffer restriction in the firmware for some Intel(R) NUC Laptop Kits before version BC0076 may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-26844	Insufficiently protected credentials in the installation binaries for Intel(R) SEAPI in all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-37049	The component tcpprep in Tcpreplay v4.4.1 was discovered to contain a heap-based buffer overflow in parse_mpls at common/get.c:150. NOTE: this is different from CVE-2022-27942.	7.8	More Details
CVE-2022-25999	Uncontrolled search path element in the Intel(R) Enpirion(R) Digital Power Configurator GUI software, all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-37048	The component tcprewrite in Tcpreplay v4.4.1 was discovered to contain a heap-based buffer overflow in get_l2len_protocol at common/get.c:344. NOTE: this is different from CVE-2022-27941.	7.8	More Details
CVE-2022-37047	The component tcprewrite in Tcpreplay v4.4.1 was discovered to contain a heap-based buffer overflow in get_ipv6_next at common/get.c:713. NOTE: this is different from CVE-2022-27940.	7.8	More Details
CVE-2021-31566	An improper link resolution flaw can occur while extracting an archive leading to changing modes, times, access control lists, and flags of a file outside of the archive. An attacker may provide a malicious archive to a victim user, who would trigger this flaw when trying to extract the archive. A local attacker may use this flaw to gain more privileges in a system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23177	An improper link resolution flaw while extracting an archive can lead to changing the access control list (ACL) of the target of the link. An attacker may provide a malicious archive to a victim user, who would trigger this flaw when trying to extract the archive. A local attacker may use this flaw to change the ACL of a file on the system and gain more privileges.	7.8	More Details
CVE-2022-28696	Uncontrolled search path in the Intel(R) Distribution for Python before version 2022.0.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-26374	Uncontrolled search path in the installation binaries for Intel(R) SEAPI all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-26344	Incorrect default permissions in the installation binaries for Intel(R) SEAPI all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-33142	Authenticated (subscriber+) Denial Of Service (DoS) vulnerability in WordPlus WordPress Better Messages plugin <= 1.9.10.57 at WordPress.	7.7	More Details
CVE-2022-36394	Authenticated (author+) SQL Injection (SQLi) vulnerability in Contest Gallery plugin <= 17.0.4 at WordPress.	7.6	More Details
CVE-2021-3513	A flaw was found in keycloak where a brute force attack is possible even when the permanent lockout feature is enabled. This is due to a wrong error message displayed when wrong credentials are entered. The highest threat from this vulnerability is to confidentiality.	7.5	More Details
CVE-2020-27793	An off-by-one overflow flaw was found in radare2 due to mismatched array length in core_java.c. This could allow an attacker to cause a crash, and perform a denail of service attack.	7.5	More Details
CVE-2022-2049	In affected versions of Octopus Deploy it is possible to perform a Regex Denial of Service via the package upload function.	7.5	More Details
CVE-2020-27795	A segmentation fault was discovered in radare2 with adf command. In libr/core/cmd_anal.c, when command "adf" has no or wrong argument, anal_fcn_data (core, input + 1) --> RAnalFunction *fcn = r_anal_get_fcn_in (core->anal, core->offset, -1); returns null pointer for fcn causing segmentation fault later in ensure_fcn_range (fcn).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30296	Insufficiently protected credentials in the Intel(R) Datacenter Group Event iOS application, all versions, may allow an unauthenticated user to potentially enable information disclosure via network access.	7.5	More Details
CVE-2022-21160	Improper buffer restrictions for some Intel(R) PROSet/Wireless WiFi products may allow an unauthenticated user to potentially enable denial of service via network access.	7.5	More Details
CVE-2022-2362	The Download Manager WordPress plugin before 3.2.50 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based download blocking restrictions.	7.5	More Details
CVE-2022-37768	libjpeg commit 281daa9 was discovered to contain an infinite loop via the component Frame::ParseTrailer.	7.5	More Details
CVE-2022-21197	Improper input validation for some Intel(R) PROSet/Wireless WiFi products may allow an unauthenticated user to potentially enable denial of service via network access.	7.5	More Details
CVE-2022-38493	Rhonabwy 0.9.99 through 1.1.x before 1.1.7 doesn't check the RSA private key length before RSA-OAEP decryption. This allows attackers to cause a Denial of Service via a crafted JWE (JSON Web Encryption) token.	7.5	More Details
CVE-2022-37422	Payara through 5.2022.2 allows directory traversal without authentication. This affects Payara Server, Payara Micro, and Payara Server Embedded.	7.5	More Details
CVE-2022-2544	The Ninja Job Board WordPress plugin before 1.3.3 does not protect the directory where it stores uploaded resumes, making it vulnerable to unauthenticated Directory Listing which allows the download of uploaded resumes.	7.5	More Details
CVE-2022-25231	The package node-opcua before 2.74.0 are vulnerable to Denial of Service (DoS) by sending a specifically crafted OPC UA message with a special OPC UA NodeID, when the requested memory allocation exceeds the v8’s memory limit.	7.5	More Details
CVE-2022-25304	All versions of package opcua; all versions of package asyncua are vulnerable to Denial of Service (DoS) due to a missing limitation on the number of received chunks - per single session or in total for all concurrent sessions. An attacker can exploit this vulnerability by sending an unlimited number of huge chunks (e.g. 2GB each) without sending the Final closing chunk.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25761	The package open62541/open62541 before 1.2.5, from 1.3-rc1 and before 1.3.1 are vulnerable to Denial of Service (DoS) due to a missing limitation on the number of received chunks - per single session or in total for all concurrent sessions. An attacker can exploit this vulnerability by sending an unlimited number of huge chunks (e.g. 2GB each) without sending the Final closing chunk.	7.5	More Details
CVE-2022-25888	The package opcua from 0.0.0 are vulnerable to Denial of Service (DoS) due to a missing limitation on the number of received chunks - per single session or in total for all concurrent sessions. An attacker can exploit this vulnerability by sending an unlimited number of huge chunks (e.g. 2GB each) without sending the Final closing chunk.	7.5	More Details
CVE-2022-35198	Contract Management System v2.0 contains a weak default password which gives attackers to access database connection information.	7.5	More Details
CVE-2022-35173	An issue was discovered in Nginx NJS v0.7.5. The JUMP offset for a break instruction was not set to a correct offset during code generation, leading to a segmentation violation.	7.5	More Details
CVE-2021-20298	A flaw was found in OpenEXR's B44Compressor. This flaw allows an attacker who can submit a crafted file to be processed by OpenEXR, to exhaust all memory accessible to the application. The highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2021-20304	A flaw was found in OpenEXR's hufDecode functionality. This flaw allows an attacker who can pass a crafted file to be processed by OpenEXR, to trigger an undefined right shift error. The highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2021-30070	An issue was discovered in HestiaCP before v1.3.5. Attackers are able to arbitrarily install packages due to values taken from the pgk [] parameter in the update request being transmitted to the operating system's package manager.	7.5	More Details
CVE-2021-3690	A flaw was found in Undertow. A buffer leak on the incoming WebSocket PONG message may lead to memory exhaustion. This flaw allows an attacker to cause a denial of service. The highest threat from this vulnerability is availability.	7.5	More Details
CVE-2021-3839	A flaw was found in the vhost library in DPDK. Function vhost_user_set_inflight_fd() does not validate `msg->payload.inflight.num_queues`, possibly causing out-of-bounds memory read/write. Any software using DPDK vhost library may crash as a result of this vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3905	A memory leak was found in Open vSwitch (OVS) during userspace IP fragmentation processing. An attacker could use this flaw to potentially exhaust available memory by keeping sending packet fragments.	7.5	More Details
CVE-2022-2547	A crafted HTTP packet without a content-type header can create a denial-of-service condition in Softing Secure Integration Server V1.22.	7.5	More Details
CVE-2022-2337	A crafted HTTP packet with a missing HTTP URI can create a denial-of-service condition in Softing Secure Integration Server V1.22.	7.5	More Details
CVE-2022-2335	A crafted HTTP packet with a -1 content-length header can create a denial-of-service condition in Softing Secure Integration Server V1.22.	7.5	More Details
CVE-2022-1748	Softing OPC UA C++ Server SDK, Secure Integration Server, edgeConnector, edgeAggregator, OPC Suite, and uaGate are affected by a NULL pointer dereference vulnerability.	7.5	More Details
CVE-2022-1069	A crafted HTTP packet with a large content-length header can create a denial-of-service condition in Softing Secure Integration Server V1.22.	7.5	More Details
CVE-2022-38149	HashiCorp Consul Template up to 0.27.2, 0.28.2, and 0.29.1 may expose the contents of Vault secrets in the error returned by the *template.Template.Execute method, when given a template using Vault secret contents incorrectly. Fixed in 0.27.3, 0.28.3, and 0.29.2.	7.5	More Details
CVE-2022-36186	A Null Pointer dereference vulnerability exists in GPAC 2.1-DEV-revUNKNOWN-master via the function gf_filter_pid_set_property_full () at filter_core/filter_pid.c:5250,which causes a Denial of Service (DoS). This vulnerability was fixed in commit b43f9d1.	7.5	More Details
CVE-2021-45454	Ampere Altra before SRP 1.08b and Altra Max before SRP 2.05 allow information disclosure of power telemetry via HWmon.	7.5	More Details
CVE-2022-25302	All versions of package asneg/opcuastack are vulnerable to Denial of Service (DoS) due to a missing handler for failed casting when unvalidated data is forwarded to boost::get function in OpcUaNodeIdBase.h. Exploiting this vulnerability is possible when sending a specifically crafted OPC UA message with a special encoded NodeId.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2074	In affected versions of Octopus Deploy it is possible to perform a Regex Denial of Service using the Variable Project Template.	7.5	More Details
CVE-2022-24381	All versions of package asneg/opcuastack are vulnerable to Denial of Service (DoS) due to a missing limitation on the number of received chunks - per single session or in total for all concurrent sessions. An attacker can exploit this vulnerability by sending an unlimited number of huge chunks (e.g. 2GB each) without sending the Final closing chunk.	7.5	More Details
CVE-2022-36024	py-cord is a an API wrapper for Discord written in Python. Bots creating using py-cord version 2.0.0 are vulnerable to remote shutdown if they are added to the server with the `application.commands` scope without the `bot` scope. Currently, it appears that all public bots that use slash commands are affected. This issue has been patched in version 2.0.1. There are currently no recommended workarounds - please upgrade to a patched version.	7.5	More Details
CVE-2022-2551	The Duplicator WordPress plugin before 1.4.7 discloses the url of the a backup to unauthenticated visitors accessing the main installer endpoint of the plugin, if the installer script has been run once by an administrator, allowing download of the full site backup without authenticating.	7.5	More Details
CVE-2022-37133	D-link DIR-816 A2_v1.10CNB04.img reboots the router without authentication via /goform/doReboot. No authentication is required, and reboot is executed when the function returns at the end.	7.5	More Details
CVE-2022-2075	In affected versions of Octopus Deploy it is possible to perform a Regex Denial of Service targeting the build information request validation.	7.5	More Details
CVE-2021-32862	The GitHub Security Lab discovered sixteen ways to exploit a cross-site scripting vulnerability in nbconvert. When using nbconvert to generate an HTML version of a user-controllable notebook, it is possible to inject arbitrary HTML which may lead to cross-site scripting (XSS) vulnerabilities if these HTML notebooks are served by a web server (eg: nbviewer).	7.5	More Details
CVE-2022-24298	All versions of package freeopcua/freeopcua are vulnerable to Denial of Service (DoS) when bypassing the limitations for excessive memory consumption by sending multiple CloseSession requests with the deleteSubscription parameter equal to False.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32778	An information disclosure vulnerability exists in the cookie functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. The session cookie and the pass cookie miss the HttpOnly flag, making them accessible via JavaScript. The session cookie also misses the secure flag, which allows the session cookie to be leaked over non-HTTPS connections. This could allow an attacker to steal the session cookie via crafted HTTP requests.This vulnerability is for the pass cookie, which contains the hashed password and can be leaked via JavaScript.	7.5	More Details
CVE-2022-37062	All FLIR AX8 thermal sensor cameras version up to and including 1.46.16 are affected by an insecure design vulnerability due to an improper directory access restriction. An unauthenticated, remote attacker can exploit this by sending a URI that contains the path of the SQLite users database and download it. A successful exploit could allow the attacker to extract usernames and hashed passwords.	7.5	More Details
CVE-2022-37060	FLIR AX8 thermal sensor cameras version up to and including 1.46.16 is vulnerable to Directory Traversal due to an improper access restriction. An unauthenticated, remote attacker can exploit this by sending a URI that contains directory traversal characters to disclose the contents of files located outside of the server's restricted path.	7.5	More Details
CVE-2022-32777	An information disclosure vulnerability exists in the cookie functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. The session cookie and the pass cookie miss the HttpOnly flag, making them accessible via JavaScript. The session cookie also misses the secure flag, which allows the session cookie to be leaked over non-HTTPS connections. This could allow an attacker to steal the session cookie via crafted HTTP requests.This vulnerabilty is for the session cookie which can be leaked via JavaScript.	7.5	More Details
CVE-2022-33916	OPC UA .NET Standard Reference Server 1.04.368 allows a remote attacker to cause the application to access sensitive information.	7.5	More Details
CVE-2022-21208	The package node-opcua before 2.74.0 are vulnerable to Denial of Service (DoS) due to a missing limitation on the number of received chunks - per single session or in total for all concurrent sessions. An attacker can exploit this vulnerability by sending an unlimited number of huge chunks (e.g. 2GB each) without sending the Final closing chunk.	7.5	More Details
CVE-2022-38668	HTTP applications (servers) based on Crow through 1.0+4 may reveal potentially sensitive uninitialized data from stack memory when fulfilling a request for a static file smaller than 16 KB.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28861	Python 3.x through 3.10 has an open redirection vulnerability in lib/http/server.py due to no protection against multiple (/) at the beginning of URI path which may leads to information disclosure. NOTE: this is disputed by a third party because the http.server.html documentation page states "Warning: http.server is not recommended for production. It only implements basic security checks."	7.4	More Details
CVE-2022-2842	A vulnerability classified as critical has been found in SourceCodester Gym Management System. This affects an unknown part of the file login.php. The manipulation of the argument user_email 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-206451.	7.3	More Details
CVE-2022-1513	A potential vulnerability was reported in Lenovo PCManager prior to version 5.0.10.4191 that may allow code execution when visiting a specially crafted website.	7.3	More Details
CVE-2022-36263	StreamLabs Desktop Application 1.9.0 is vulnerable to Incorrect Access Control via obs64.exe. An attacker can execute arbitrary code via a crafted .exe file.	7.3	More Details
CVE-2022-29549	An issue was discovered in Qualys Cloud Agent 4.8.0-49. It executes programs at various full pathnames without first making ownership and permission checks (e.g., to help ensure that a program was installed by root) and without integrity checks (e.g., a checksum comparison against known legitimate programs). Also, the vendor recommendation is to install this agent software with root privileges. Thus, privilege escalation is possible on systems where any of these pathnames is controlled by a non-root user. An example is /opt/firebird/bin/isql, where the /opt/firebird directory is often owned by the firebird user.	7.3	More Details
CVE-2022-25811	The Transposh WordPress Translation WordPress plugin through 1.0.8 does not sanitise and escape the order and orderby parameters before using them in a SQL statement, leading to a SQL injection	7.2	More Details
CVE-2022-2593	The Better Search Replace WordPress plugin before 1.4.1 does not properly sanitise and escape table data before inserting it into a SQL query, which could allow high privilege users to perform SQL Injection attacks	7.2	More Details
CVE-2022-36215	DedeBIZ v6 was discovered to contain a remote code execution vulnerability in sys_info.php.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36216	DedeCMS v5.7.94 - v5.7.97 was discovered to contain a remote code execution vulnerability in member_toadmin.php.	7.2	More Details
CVE-2022-32579	Improper initialization in the firmware for some Intel(R) NUC Laptop Kits before version BC0076 may allow a privileged user to potentially enable escalation of privilege via physical access.	7.2	More Details
CVE-2022-35203	An access control issue in TrendNet TV-IP572PI v1.0 allows unauthenticated attackers to access sensitive system information.	7.2	More Details
CVE-2022-1373	The “restore configuration” feature of Softing Secure Integration Server V1.22 is vulnerable to a directory traversal vulnerability when processing zip files. An attacker can craft a zip file to load an arbitrary dll and execute code. Using the "restore configuration" feature to upload a zip file containing a path traversal file may cause a file to be created and executed upon touching the disk.	7.2	More Details
CVE-2022-2334	The application searches for a library dll that is not found. If an attacker can place a dll with this name, then the attacker can leverage it to execute arbitrary code on the targeted Softing Secure Integration Server V1.22.	7.2	More Details
CVE-2022-25812	The Transposh WordPress Translation WordPress plugin before 1.0.8 does not validate its debug settings, which could allow allowing high privilege users such as admin to perform RCE	7.2	More Details
CVE-2022-36285	Authenticated Arbitrary File Upload vulnerability in dmitrylitvinov Uploading SVG, WEBP and ICO files plugin <= 1.0.1 at WordPress.	7.2	More Details
CVE-2021-37289	Insecure Permissions in administration interface in Planex MZK-DP150N 1.42 and 1.43 allows attackers to execute system command as root via etc_ro/web/syscmd.asp.	7.2	More Details
CVE-2022-34486	Path traversal vulnerability in PukiWiki versions 1.4.5 to 1.5.3 allows a remote authenticated attacker with an administrative privilege to execute a malicious script via unspecified vectors.	7.2	More Details
CVE-2020-27792	A heap-based buffer overwrite vulnerability was found in GhostScript's lp8000_print_page() function in the gdevlp8k.c file. This flaw allows an attacker to trick a user into opening a crafted PDF file, triggering the heap buffer overflow that could lead to memory corruption or a denial of service.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3481	A flaw was found in Qt. An out-of-bounds read vulnerability was found in QRadialFetchSimd in qt/qtbase/src/gui/painting/qdrawhelper_p.h in Qt/Qtbase. While rendering and displaying a crafted Scalable Vector Graphics (SVG) file this flaw may lead to an unauthorized memory access. The highest threat from this vulnerability is to data confidentiality and the application availability.	7.1	More Details
CVE-2022-36008	Frontier is Substrate's Ethereum compatibility layer. A security issue was discovered affecting parsing of the RPC result of the exit reason in case of EVM reversion. In release build, this would cause the exit reason being incorrectly parsed and returned by RPC. In debug build, this would cause an overflow panic. No action is needed unless you have a bridge node that needs to distinguish different reversion exit reasons and you used RPC for this. There are currently no known workarounds.	7.1	More Details
CVE-2022-1400	Use of Hard-coded Cryptographic Key vulnerability in the WebReportsApi.dll of Exago Web Reports, as used in the Device42 Asset Management Appliance, allows an attacker to leak session IDs and elevate privileges. This issue affects: Device42 CMDB versions prior to 18.01.00.	7.1	More Details
CVE-2021-23179	Out of bounds read in firmware for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products before version 22.120 may allow a privileged user to potentially enable information disclosure via local access.	7.1	More Details
CVE-2022-36023	Hyperledger Fabric is an enterprise-grade permissioned distributed ledger framework for developing solutions and applications. If a gateway client application sends a malformed request to a gateway peer it may crash the peer node. Version 2.4.6 checks for the malformed gateway request and returns an error to the gateway client. There are no known workarounds, users must upgrade to version 2.4.6.	7.0	More Details
CVE-2022-1401	Improper Access Control vulnerability in the /Exago/WrImageResource.adx route as used in Device42 Asset Management Appliance allows an unauthenticated attacker to read sensitive server files with root permissions. This issue affects: Device42 CMDB versions prior to 18.01.00.	6.9	More Details
CVE-2021-20316	A flaw was found in the way Samba handled file/directory metadata. This flaw allows an authenticated attacker with permissions to read or modify share metadata, to perform this operation outside of the share.	6.8	More Details
CVE-2022-28697	Improper access control in firmware for Intel(R) AMT and Intel(R) Standard Manageability may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3827	A flaw was found in keycloak, where the default ECP binding flow allows other authentication flows to be bypassed. By exploiting this behavior, an attacker can bypass the MFA authentication by sending a SOAP request with an AuthnRequest and Authorization header with the user's credentials. The highest threat from this vulnerability is to confidentiality and integrity.	6.8	More Details
CVE-2022-21172	Out of bounds write for some Intel(R) PROSet/Wireless WiFi products may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-3701	A flaw was found in ansible-runner where the default temporary files configuration in ansible-2.0.0 are written to world R/W locations. This flaw allows an attacker to pre-create the directory, resulting in reading private information or forcing ansible-runner to write files as the legitimate user in a place they did not expect. The highest threat from this vulnerability is to confidentiality and integrity.	6.6	More Details
CVE-2022-2792	Emerson Electric's Proficy Machine Edition Version 9.00 and prior is vulenrable to CWE-284 Improper Access Control, and stores project data in a directory with improper access control lists.	6.6	More Details
CVE-2022-21212	Improper input validation for some Intel(R) PROSet/Wireless WiFi products may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2022-35191	D-Link Wireless AC1200 Dual Band VDSL ADSL Modem Router DSL-3782 Firmware v1.01 allows unauthenticated attackers to cause a Denial of Service (DoS) via a crafted HTTP connection request.	6.5	More Details
CVE-2022-28710	An information disclosure vulnerability exists in the chunkFile functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary file read. An attacker can send an HTTP request to trigger this vulnerability.	6.5	More Details
CVE-2021-23168	Out of bounds read for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi products may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35992	Fiserv Prologue through 2020-12-16 does not properly protect the database password. If an attacker were to gain access to the configuration file (specifically, the LogPassword attribute within appconfig.ini), they would be able to decrypt the password stored within the configuration file. This would yield cleartext credentials for the database (to gain access to financial records of customers stored within the database), and in some cases would allow remote login to the database.	6.5	More Details
CVE-2022-32453	HTTP header injection vulnerability in Cybozu Office 10.0.0 to 10.8.5 may allow a remote attacker to obtain and/or alter the data of the product via unspecified vectors.	6.5	More Details
CVE-2022-2568	A privilege escalation flaw was found in the Ansible Automation Platform. This flaw allows a remote authenticated user with 'change user' permissions to modify the account settings of the superuser account and also remove the superuser privileges.	6.5	More Details
CVE-2022-36031	Directus is a free and open-source data platform for headless content management. The Directus process can be aborted by having an authorized user update the `filename_disk` value to a folder and accessing that file through the `/assets` endpoint. This vulnerability has been patched and release v9.15.0 contains the fix. Users are advised to upgrade. Users unable to upgrade may prevent this problem by making sure no (untrusted) non-admin users have permissions to update the `filename_disk` field on `directus_files`.	6.5	More Details
CVE-2021-3670	MaxQueryDuration not honoured in Samba AD DC LDAP	6.5	More Details
CVE-2022-32761	An information disclosure vulnerability exists in the aVideoEncoderReceiveImage functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary file read. An attacker can send an HTTP request to trigger this vulnerability.	6.5	More Details
CVE-2022-25228	CandidATS Version 3.0.0 Beta allows an authenticated user to inject SQL queries in '/index.php?m=settings&a=show' via the 'userID' parameter, in '/index.php?m=candidates&a=show' via the 'candidateID', in '/index.php?m=joborders&a=show' via the 'jobOrderID' and '/index.php?m=companies&a=show' via the 'companyID' parameter	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25810	The Transposh WordPress Translation WordPress plugin through 1.0.8 exposes a couple of sensitive actions such has “tp_reset” under the Utilities tab (/wp-admin/admin.php?page=tp_utils), which can be used/executed as the lowest-privileged user. Basically all Utilities functionalities are vulnerable this way, which involves resetting configurations and backup/restore operations.	6.5	More Details
CVE-2022-37428	PowerDNS Recursor up to and including 4.5.9, 4.6.2 and 4.7.1, when protobuf logging is enabled, has Improper Cleanup upon a Thrown Exception, leading to a denial of service (daemon crash) via a DNS query that leads to an answer with specific properties.	6.5	More Details
CVE-2022-38663	Jenkins Git Plugin 4.11.4 and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log provided by the Git Username and Password (`gitUsernamePassword`) credentials binding.	6.5	More Details
CVE-2022-2555	The Yotpo Reviews for WooCommerce WordPress plugin through 2.0.4 lacks nonce check when updating its settings, which could allow attacker to make a logged in admin change them via a CSRF attack.	6.5	More Details
CVE-2022-34621	Mealie 1.0.0beta3 was discovered to contain an Insecure Direct Object Reference (IDOR) vulnerability which allows attackers to modify user passwords and other attributes via modification of the user_id parameter.	6.5	More Details
CVE-2022-35242	Unauthenticated plugin settings change vulnerability in 59sec THE Leads Management System: 59sec LITE plugin <= 3.4.1 at WordPress.	6.5	More Details
CVE-2022-35148	maccms10 v2021.1000.1081 to v2022.1000.3031 was discovered to contain a SQL injection vulnerability via the table parameter at database/columns.html.	6.5	More Details
CVE-2022-2392	The Lana Downloads Manager WordPress plugin before 1.8.0 is affected by an arbitrary file download vulnerability that can be exploited by users with "Contributor" permissions or higher.	6.5	More Details
CVE-2022-2388	The WP Coder WordPress plugin before 2.5.3 does not have CSRF check in place when deleting code created by the plugin, which could allow attackers to make a logged in admin delete arbitrary ones via a CSRF attack	6.5	More Details
CVE-2022-37770	libjpeg commit 281daa9 was discovered to contain a segmentation fault via LineMerger::GetNextLowpassLine at linemerger.cpp. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted file.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37769	libjpeg commit 281daa9 was discovered to contain a segmentation fault via HuffmanDecoder::Get at huffmandecoder.hpp. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted file.	6.5	More Details
CVE-2022-38665	Jenkins CollabNet Plugins Plugin 2.0.8 and earlier stores a RabbitMQ password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2021-44545	Improper input validation for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi products may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2021-3975	A use-after-free flaw was found in libvirt. The qemuMonitorUnregister() function in qemuProcessHandleMonitorEOF is called using multiple threads without being adequately protected by a monitor lock. This flaw could be triggered by the virConnectGetAllDomainStats API when the guest is shutting down. An unprivileged client with a read-only connection could use this flaw to perform a denial of service attack by causing the libvirt daemon to crash.	6.5	More Details
CVE-2021-3702	A race condition flaw was found in ansible-runner, where an attacker could watch for rapid creation and deletion of a temporary directory, substitute their directory at that name, and then have access to ansible-runner's private_data_dir the next time ansible-runner made use of the private_data_dir. The highest Threat out of this flaw is to integrity and confidentiality.	6.3	More Details
CVE-2022-34774	Tabit - Arbitrary account modification. One of the endpoints mapped by the tiny URL, was a page where an adversary can modify personal details, such as email addresses and phone numbers of a specific user in a restaurant's loyalty program. Possibly allowing account takeover (the mail can be used to reset password).	6.3	More Details
CVE-2022-34775	Tabit - Excessive data exposure. Another endpoint mapped by the tiny url, was one for reservation cancellation, containing the MongoDB ID of the reservation, and organization. This can be used to query the http://tgm-api.tabit.cloud/rsv/management/{reservationId}?organization={orgId} API which returns a lot of data regarding the reservation (OWASP: API3): Name, mail, phone number, the number of visits of the user to this specific restaurant, the money he spent there, the money he spent on alcohol, whether he left a deposit etc. This information can easily be used for a phishing attack.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2909	A vulnerability was found in SourceCodester Simple and Nice Shopping Cart Script. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /mkshop/Men/profile.php. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206845 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2876	A vulnerability, which was classified as critical, was found in SourceCodester Student Management System. Affected is an unknown function of the file index.php. The manipulation of the argument 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-206634 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-34345	Improper input validation in the firmware for some Intel(R) NUC Laptop Kits before version BC0076 may allow a privileged user to potentially enable escalation of privilege via physical access.	6.2	More Details
CVE-2022-29476	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability in 8 Degree Themes otification Bar for WordPress plugin <= 1.1.8 at WordPress.	6.1	More Details
CVE-2021-3639	A flaw was found in mod_auth_mellon where it does not sanitize logout URLs properly. This issue could be used by an attacker to facilitate phishing attacks by tricking users into visiting a trusted web application URL that redirects to an external and potentially malicious server. The highest threat from this liability is to confidentiality and integrity.	6.1	More Details
CVE-2019-25075	HTML injection combined with path traversal in the Email service in Gravitee API Management before 1.25.3 allows anonymous users to read arbitrary files via a /management/users/register request.	6.1	More Details
CVE-2022-35151	kkFileView v4.1.0 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities via the urls and currentUrl parameters at /controller/OnlinePreviewController.java.	6.1	More Details
CVE-2022-35212	osCommerce2 before v2.3.4.1 was discovered to contain a cross-site scripting (XSS) vulnerability via the function tep_db_error().	6.1	More Details
CVE-2022-30604	Cross-site scripting vulnerability in the specific parameters of Cybozu Office 10.0.0 to 10.8.5 allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1932	The Rezgo Online Booking WordPress plugin before 4.1.8 does not sanitise and escape some parameters before outputting them back in a page, leading to a Reflected Cross-Site Scripting, which can be exploited either via a LFI in an AJAX action, or direct call to the affected file	6.1	More Details
CVE-2022-35278	In Apache ActiveMQ Artemis prior to 2.24.0, an attacker could show malicious content and/or redirect users to a malicious URL in the web console by using HTML in the name of an address or queue.	6.1	More Details
CVE-2022-35213	Ecommerce-CodeIgniter-Bootstrap before commit 56465f was discovered to contain a cross-site scripting (XSS) vulnerability via the function base_url() at /blog/blogpublish.php.	6.1	More Details
CVE-2021-30071	A cross-site scripting (XSS) vulnerability in /admin/list_key.html of HestiaCP before v1.3.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2022-2383	The Feed Them Social WordPress plugin before 3.0.1 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-2022-28598	Frappe ERPNext 12.29.0 is vulnerable to XSS where the software does not neutralize or incorrectly neutralize user-controllable input before it is placed in output that is used as a web page that is served to other users.	6.1	More Details
CVE-2022-38463	ServiceNow through San Diego Patch 4b and Patch 6 allows reflected XSS in the logout functionality.	6.1	More Details
CVE-2022-38172	ServiceNow through San Diego Patch 3 allows XSS via the name field during creation of a new dashboard for the Performance Analytics dashboard.	6.1	More Details
CVE-2022-2532	The Feed Them Social WordPress plugin before 3.0.1 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-2022-33151	Cross-site scripting vulnerability in the specific parameters of Cybozu Office 10.0.0 to 10.8.5 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2022-34857	Reflected Cross-Site Scripting (XSS) vulnerability in smartypants SP Project & Document Manager plugin <= 4.59 at WordPress	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24910	The Transposh WordPress Translation WordPress plugin before 1.0.8 does not sanitise and escape the a parameter via an AJAX action (available to both unauthenticated and authenticated users when the curl library is installed) before outputting it back in the response, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2022-36251	Clinic's Patient Management System v1.0 is vulnerable to Cross Site Scripting (XSS) via patients.php.	6.1	More Details
CVE-2022-27637	Reflected cross-site scripting vulnerability in PukiWiki versions 1.5.1 to 1.5.3 allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2022-32772	A cross-site scripting (xss) vulnerability exists in the footer alerts functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.This vulnerability arrises from the "msg" parameter which is inserted into the document with insufficient sanitization.	6.1	More Details
CVE-2022-32771	A cross-site scripting (xss) vulnerability exists in the footer alerts functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.This vulnerability arrises from the "success" parameter which is inserted into the document with insufficient sanitization.	6.1	More Details
CVE-2022-32770	A cross-site scripting (xss) vulnerability exists in the footer alerts functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.This vulnerability arrises from the "toast" parameter which is inserted into the document with insufficient sanitization.	6.1	More Details
CVE-2022-2932	Cross-site Scripting (XSS) - Reflected in GitHub repository bustle/mobiledoc-kit prior to 0.14.2.	6.1	More Details
CVE-2022-0542	Cross-site Scripting (XSS) - DOM in GitHub repository chatwoot/chatwoot prior to 2.7.0.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35133	A cross-site scripting (XSS) vulnerability in CherryTree v0.99.30 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name text field when creating a node.	6.1	More Details
CVE-2022-35554	Multiple reflected XSS vulnerabilities occur when handling error message of BPC SmartVista version 3.28.0 allowing an attacker to execute javascript code at client side.	6.1	More Details
CVE-2022-35654	Pega Platform from 8.5.4 to 8.7.3 is affected by an XSS issue with an unauthenticated user and the redirect parameter.	6.1	More Details
CVE-2022-35655	Pega Platform from 7.3 to 8.7.3 is affected by an XSS issue due to a misconfiguration of a datapage setting.	6.1	More Details
CVE-2022-28715	Cross-site scripting vulnerability in the specific parameters of Cybozu Office 10.0.0 to 10.8.5 allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2022-30690	A cross-site scripting (xss) vulnerability exists in the image403 functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.	6.1	More Details
CVE-2022-29487	Cross-site scripting vulnerability in Cybozu Office 10.0.0 to 10.8.5 allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2022-34624	Mealie1.0.0beta3 does not terminate download tokens after a user logs out, allowing attackers to perform a man-in-the-middle attack via a crafted GET request.	5.9	More Details
CVE-2022-1930	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the eth-account PyPI package, when an attacker is able to supply arbitrary input to the encode_structured_data method	5.9	More Details
CVE-2022-2790	Emerson Electric's Proficy Machine Edition Version 9.00 and prior is vulenrable to CWE-347 Improper Verification of Cryptographic Signature, and does not properly verify compiled logic (PDT files) and data blocks data (BLD/BLK files).	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23460	Jsonxx or Json++ is a JSON parser, writer and reader written in C++. In affected versions of jsonxx json parsing may lead to stack exhaustion in an address sanitized (ASAN) build. This issue may lead to Denial of Service if the program using the jsonxx library crashes. This issue exists on the current commit of the jsonxx project and the project itself has been archived. Updates are not expected. Users are advised to find a replacement.	5.9	More Details
CVE-2022-2793	Emerson Electric's Proficy Machine Edition Version 9.00 and prior is vulenrable to CWE-353 Missing Support for Integrity Check, and has no authentication or authorization of data packets after establishing a connection for the SRTP protocol.	5.9	More Details
CVE-2021-3714	A flaw was found in the Linux kernels memory deduplication mechanism. Previous work has shown that memory deduplication can be attacked via a local exploitation mechanism. The same technique can be used if an attacker can upload page sized files and detect the change in access time from a networked service to determine if the page has been merged.	5.9	More Details
CVE-2022-2338	Softing Secure Integration Server V1.22 is vulnerable to authentication bypass via a machine-in-the-middle attack. The default the administration interface is accessible via plaintext HTTP protocol, facilitating the attack. The HTTP request may contain the session cookie in the request, which may be captured for use in authenticating to the server.	5.7	More Details
CVE-2021-3800	A flaw was found in glib before version 2.63.6. Due to random charset alias, pkexec can leak content from files owned by privileged users to unprivileged ones under the right condition.	5.5	More Details
CVE-2022-35165	An issue in AP4_SgpdAtom::AP4_SgpdAtom() of Bento4-1.6.0-639 allows attackers to cause a Denial of Service (DoS) via a crafted mp4 input.	5.5	More Details
CVE-2020-27787	A Segmentaation fault was found in UPX in invert_pt_dynamic() function in p_lx_elf.cpp. An attacker with a crafted input file allows invalid memory address access that could lead to a denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34776	Tabit - giftcard stealth. Several APIs on the web system display, without authorization, sensitive information such as health statements, previous bills in a specific restaurant, alcohol consumption and smoking habits. Each of the described APIs, has in its URL one or more MongoDB ID which is not so simple to enumerate. However, they each receive a 'tiny URL' in tabits domain, in the form of https://tbit.be/{suffix} with suffix being a 5 character long string containing numbers, lower and upper case letters. It is not so simple to enumerate them all, but really easy to find some that work and lead to a personal endpoint. Furthermore, the redirect URL disclosed the MongoDB IDs discussed above, and we could use them to query other endpoints disclosing more personal information.	5.5	More Details
CVE-2022-2869	libtiff's tiffcrop tool has a uint32_t underflow which leads to out of bounds read and write in the extractContigSamples8bits routine. An attacker who supplies a crafted file to tiffcrop could trigger this flaw, most likely by tricking a user into opening the crafted file with tiffcrop. Triggering this flaw could cause a crash or potentially further exploitation.	5.5	More Details
CVE-2020-27790	A floating point exception issue was discovered in UPX in PackLinuxElf64::invert_pt_dynamic() function of p_lx_elf.cpp file. An attacker with a crafted input file could trigger this issue that could cause a crash leading to a denial of service. The highest impact is to Availability.	5.5	More Details
CVE-2021-26254	Out of bounds read for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi products may allow a privileged user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-27788	An out-of-bounds read access vulnerability was discovered in UPX in PackLinuxElf64::canPack() function of p_lx_elf.cpp file. An attacker with a crafted input file could trigger this issue that could cause a crash leading to a denial of service.	5.5	More Details
CVE-2022-2868	libtiff's tiffcrop utility has a improper input validation flaw that can lead to out of bounds read and ultimately cause a crash if an attacker is able to supply a crafted file to tiffcrop.	5.5	More Details
CVE-2021-3736	A flaw was found in the Linux kernel. A memory leak problem was found in mbochs_ioctl in samples/vfio-mdev/mbochs.c in Virtual Function I/O (VFIO) Mediated devices. This flaw could allow a local attacker to leak internal kernel information.	5.5	More Details
CVE-2022-2923	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0240.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3759	A memory overflow vulnerability was found in the Linux kernel's ipc functionality of the memcg subsystem, in the way a user calls the semget function multiple times, creating semaphores. This flaw allows a local user to starve the resources, causing a denial of service. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2022-2867	libtiff's tiffcrop utility has a uint32_t underflow that can lead to out of bounds read and write. An attacker who supplies a crafted file to tiffcrop (likely via tricking a user to run tiffcrop on it with certain parameters) could cause a crash or in some cases, further exploitation.	5.5	More Details
CVE-2022-2874	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0224.	5.5	More Details
CVE-2021-3764	A memory leak flaw was found in the Linux kernel's ccp_run_aes_gcm_cmd() function that allows an attacker to cause a denial of service. The vulnerability is similar to the older CVE-2019-18808. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2021-3798	A flaw was found in openCryptoki. The openCryptoki Soft token does not check if an EC key is valid when an EC key is created via C_CreateObject, nor when C_DeriveKey is used with ECDH public data. This may allow a malicious user to extract the private key by performing an invalid curve attack.	5.5	More Details
CVE-2022-29550	An issue was discovered in Qualys Cloud Agent 4.8.0-49. It writes "ps auxwwe" output to the /var/log/qualys/qualys-cloud-agent-scan.log file. This may, for example, unexpectedly write credentials (from environment variables) to disk in cleartext. NOTE: there are no common circumstances in which qualys-cloud-agent-scan.log can be read by a user other than root; however, the file contents could be exposed through site-specific operational practices. The vendor does NOT characterize this as a vulnerability because the ps data collection is intentional, and would only capture credentials on a machine that was already affected by the CWE-214 weakness	5.5	More Details
CVE-2022-2873	An out-of-bounds memory access flaw was found in the Linux kernel Intel's iSMT SMBus host controller driver in the way a user triggers the I2C_SMBUS_BLOCK_DATA (with the ioctl I2C_SMBUS) with malicious input data. This flaw allows a local user to crash the system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21793	Insufficient control flow management in the Intel(R) Ethernet 500 Series Controller drivers for VMWare before version 1.11.4.0 and in the Intel(R) Ethernet 700 Series Controller drivers for VMWare before version 2.1.5.0 may allow an authenticated user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2022-21233	Improper isolation of shared resources in some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-29507	Insufficiently protected credentials in the Intel(R) Team Blue mobile application in all versions may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-36191	A heap-buffer-overflow had occurred in function gf_isom_dovi_config_get of isomedia/avc_ext.c:2490, as demonstrated by MP4Box. This vulnerability was fixed in commit fef6242.	5.5	More Details
CVE-2021-3917	A flaw was found in the coreos-installer, where it writes the Ignition config to the target system with world-readable access permissions. This flaw allows a local attacker to have read access to potentially sensitive data. The highest threat from this vulnerability is to confidentiality.	5.5	More Details
CVE-2021-44470	Incorrect default permissions for the Intel(R) Connect M Android application before version 1.7.4 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2021-3997	A flaw was found in systemd. An uncontrolled recursion in systemd-tmpfiles may lead to a denial of service at boot time when too many nested directories are created in /tmp.	5.5	More Details
CVE-2022-27500	Incorrect default permissions for the Intel(R) Support Android application before 21.07.40 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-26373	Non-transparent sharing of return predictor targets between contexts in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-30944	Insufficiently protected credentials for Intel(R) AMT and Intel(R) Standard Manageability may allow a privileged user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-21140	Improper access control for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi products may allow a privileged user to potentially enable information disclosure via local access.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21152	Improper access control in the Intel(R) Edge Insights for Industrial software before version 2.6.1 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2021-3996	A logic error was found in the libmount library of util-linux in the function that allows an unprivileged user to unmount a FUSE filesystem. This flaw allows a local user on a vulnerable system to unmount other users' filesystems that are either world-writable themselves (like /tmp) or mounted in a world-writable directory. An attacker may use this flaw to cause a denial of service to applications that use the affected filesystems.	5.5	More Details
CVE-2021-3659	A NULL pointer dereference flaw was found in the Linux kernel's IEEE 802.15.4 wireless networking subsystem in the way the user closes the LR-WPAN connection. This flaw allows a local user to crash the system. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2022-24378	Improper initialization in the Intel(R) Data Center Manager software before version 4.1 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2022-23403	Improper input validation in the Intel(R) Data Center Manager software before version 4.1 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-26950	Out of bounds read in firmware for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products before version 22.120 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-26257	Improper buffer restrictions in firmware for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products before version 22.120 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-3995	A logic error was found in the libmount library of util-linux in the function that allows an unprivileged user to unmount a FUSE filesystem. This flaw allows an unprivileged local attacker to unmount FUSE filesystems that belong to certain other users who have a UID that is a prefix of the UID of the attacker in its string form. An attacker may use this flaw to cause a denial of service to applications that use the affected filesystems.	5.5	More Details
CVE-2022-35166	libjpeg commit 842c7ba was discovered to contain an infinite loop via the component JPEG::ReadInternal.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34771	Tabit - arbitrary SMS send on Tabits behalf. The resend OTP API of tabit allows an adversary to send messages on tabits behalf to anyone registered on the system - the API receives the parameters: phone number, and CustomMessage, We can use that API to craft malicious messages to any user of the system. In addition, the API probably has some kind of template injection potential. When entering {{OTP}} in the custom message field it is formatted into an OTP.	5.5	More Details
CVE-2022-36233	Tenda AC9 V15.03.2.13 is vulnerable to Buffer Overflow via httpd, form_fast_setting_wifi_set. httpd.	5.5	More Details
CVE-2022-2375	The WP Sticky Button WordPress plugin before 1.4.1 does not have authorisation and CSRF checks when saving its settings, allowing unauthenticated users to update them. Furthermore, due to the lack of escaping in some of them, it could lead to Stored Cross-Site Scripting issues	5.4	More Details
CVE-2021-3442	A flaw was found in the Red Hat OpenShift API Management product. User input is not validated allowing an authenticated user to inject scripts into some text boxes leading to a XSS attack. The highest threat from this vulnerability is to data confidentiality.	5.4	More Details
CVE-2022-35174	A stored cross-site scripting (XSS) vulnerability in Kirby's Starterkit v3.7.0.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Tags field.	5.4	More Details
CVE-2022-37063	All FLIR AX8 thermal sensor cameras versions up to and including 1.46.16 are vulnerable to Cross Site Scripting (XSS) due to improper input sanitization. An authenticated remote attacker can execute arbitrary JavaScript code in the web management interface. A successful exploit could allow the attacker to insert malicious JavaScript code.	5.4	More Details
CVE-2021-24912	The Transposh WordPress Translation WordPress plugin before 1.0.8 does not have CSRF check in its tp_translation AJAX action, which could allow attackers to make authorised users add a translation. Given the lack of sanitisation in the tk0 parameter, this could lead to a Stored Cross-Site Scripting issue which will be executed in the context of a logged in admin	5.4	More Details
CVE-2021-24911	The Transposh WordPress Translation WordPress plugin before 1.0.8 does not sanitise and escape the tk0 parameter from the tp_translation AJAX action, leading to Stored Cross-Site Scripting, which will trigger in the admin dashboard of the plugin. The minimum role needed to perform such attack depends on the plugin "Who can translate ?" setting.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2890	Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.	5.4	More Details
CVE-2022-2312	The Student Result or Employee Database WordPress plugin before 1.7.5 does not have CSRF in its AJAX actions, allowing attackers to make logged in user with a role as low as contributor to add/edit and delete students via CSRF attacks. Furthermore, due to the lack of sanitisation and escaping, it could also lead to Stored Cross-Site scripting	5.4	More Details
CVE-2022-1021	Insecure Storage of Sensitive Information in GitHub repository chatwoot/chatwoot prior to 2.6.0.	5.4	More Details
CVE-2022-2829	Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.	5.4	More Details
CVE-2022-35910	In Jellyfin before 10.8, stored XSS allows theft of an admin access token.	5.4	More Details
CVE-2020-35509	A flaw was found in keycloak affecting versions 11.0.3 and 12.0.0. An expired certificate would be accepted by the direct-grant authenticator because of missing time stamp validations. The highest threat from this vulnerability is to data confidentiality and integrity.	5.4	More Details
CVE-2022-2600	The Auto-hyperlink URLs WordPress plugin through 5.4.1 does not set rel="noopener noreferer" on generated links, which can lead to Tab Nabbing by giving the target site access to the source tab through the window.opener DOM object.	5.4	More Details
CVE-2022-36405	Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in amCharts: Charts and Maps plugin <= 1.4 at WordPress.	5.4	More Details
CVE-2022-36350	Stored cross-site scripting vulnerability in PukiWiki versions 1.3.1 to 1.5.3 allows a remote attacker to inject an arbitrary script via unspecified vectors.	5.4	More Details
CVE-2022-36341	Authenticated (subscriber+) plugin settings change leading to Stored Cross-Site Scripting (XSS) vulnerability in Akash soni's AS – Create Pinterest Pinboard Pages plugin <= 1.0 at WordPress.	5.4	More Details
CVE-2022-36292	Cross-Site Request Forgery (CSRF) vulnerabilities in WPChill Gallery PhotoBlocks plugin <= 1.2.6 at WordPress.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36288	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.	5.4	More Details
CVE-2022-38664	Jenkins Job Configuration History Plugin 1165.v8cc9fd1f4597 and earlier does not escape the job name on the System Configuration History page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to configure job names.	5.4	More Details
CVE-2020-23466	Cross Site Scripting (XSS) vulnerability exists in the phpgurukul Online Marriage Registration System 1.0 allows attackers to run arbitrary code via the wzipcode field.	5.4	More Details
CVE-2022-2871	Cross-site Scripting (XSS) - Stored in GitHub repository notrinos/notrinoserp prior to 0.7.	5.4	More Details
CVE-2022-37254	DolphinPHP 1.5.1 is vulnerable to Cross Site Scripting (XSS) via Background - > System - > system function - > configuration management.	5.4	More Details
CVE-2022-34658	Multiple Authenticated (contributor+) Persistent Cross-Site Scripting (XSS) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.	5.4	More Details
CVE-2022-1340	Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.	5.4	More Details
CVE-2022-35692	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to leak minor information of another user's account detials. Exploitation of this issue does not require user interaction.	5.3	More Details
CVE-2022-2552	The Duplicator WordPress plugin before 1.4.7 does not authenticate or authorize visitors before displaying information about the system such as server software, php version and full file system path to the site.	5.3	More Details
CVE-2022-33932	Dell PowerScale OneFS, versions 9.0.0 up to and including 9.1.0.19, 9.2.1.12, 9.3.0.6, and 9.4.0.2, contain an unprotected primary channel vulnerability. An unauthenticated network malicious attacker may potentially exploit this vulnerability, leading to a denial of filesystem services.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1901	In affected versions of Octopus Deploy it is possible to unmask sensitive variables by using variable preview.	5.3	More Details
CVE-2022-2558	The Simple Job Board WordPress plugin before 2.10.0 is susceptible to Directory Listing which allows the public listing of uploaded resumes in certain configurations.	5.3	More Details
CVE-2022-30693	Information disclosure vulnerability in the system configuration of Cybozu Office 10.0.0 to 10.8.5 allows a remote attacker to obtain the data of the product via unspecified vectors.	5.3	More Details
CVE-2022-1989	All CODESYS Visualization versions before V4.2.0.0 generate a login dialog vulnerable to information exposure allowing a remote, unauthenticated attacker to enumerate valid users.	5.3	More Details
CVE-2022-38392	Certain 5400 RPM hard drives, for laptops and other PCs in approximately 2005 and later, allow physically proximate attackers to cause a denial of service (device malfunction and system crash) via a resonant-frequency attack with the audio signal from the Rhythm Nation music video. A reported product is Seagate STDT4000100 763649053447.	5.3	More Details
CVE-2022-35976	The GitOps Tools Extension for VSCode relies on kubeconfigs in order to communicate with Kubernetes clusters. A specially crafted kubeconfig leads to arbitrary code execution on behalf of the user running VSCode. Users relying on kubeconfigs that are generated or altered by other processes or users are affected by this issue. Please note that the vulnerability is specific to this extension, and the same kubeconfig would not result in arbitrary code execution when used with kubectl. Using only trust-worthy kubeconfigs is a safe mitigation. However, updating to the latest version of the extension is still highly recommended.	5.2	More Details
CVE-2022-36009	gomatrixserverlib is a Go library for matrix protocol federation. Dendrite is a Matrix homeserver written in Go, an alternative to Synapse. The power level parsing within gomatrixserverlib was failing to parse the `"events_default"` key of the `m.room.power_levels` event, defaulting the event default power level to zero in all cases. Power levels are the matrix terminology for user access level. In rooms where the `"events_default"` power level had been changed, this could result in events either being incorrectly authorised or rejected by Dendrite servers. gomatrixserverlib contains a fix as of commit `723fd49` and Dendrite 0.9.3 has been updated accordingly. Matrix rooms where the `"events_default"` power level has not been changed from the default of zero are not vulnerable. Users are advised to upgrade. There are no known workarounds for this issue.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2886	A vulnerability, which was classified as critical, was found in Laravel 5.1. Affected is an unknown function. The manipulation leads to deserialization. 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-206688.	5.0	More Details
CVE-2022-32769	Multiple authentication bypass vulnerabilities exist in the objects id handling functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request by an authenticated user can lead to unauthorized access and takeover of resources. An attacker can send an HTTP request to trigger this vulnerability.This vulnerability exists in the Playlists plugin, allowing an attacker to bypass authentication by guessing a sequential ID, allowing them to take over the another user's playlists.	5.0	More Details
CVE-2022-34773	Tabit - HTTP Method manipulation. https://bridge.tabit.cloud/configuration/addresses-query - can be POST-ed to add addresses to the DB. This is an example of OWASP:API8 – Injection.	4.9	More Details
CVE-2022-35235	Authenticated (admin+) Arbitrary File Read vulnerability in XplodedThemes WPide plugin <= 2.6 at WordPress.	4.9	More Details
CVE-2021-29891	IBM OPENBMC OP910 and OP940 could allow a privileged user to upload an improper site identity certificate that may cause it to lose network services. IBM X-Force ID: 207221.	4.9	More Details
CVE-2022-2361	The WP Social Chat WordPress plugin before 6.0.5 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.	4.8	More Details
CVE-2022-2796	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.4.	4.8	More Details
CVE-2022-36347	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alpine Press Alpine PhotoTile for Pinterest plugin <= 1.3.1 at WordPress.	4.8	More Details
CVE-2022-36282	Authenticated (editor+) Stored Cross-Site Scripting (XSS) vulnerability in Roman Pronskiy's Search Exclude plugin <= 1.2.6 at WordPress.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34648	Authenticated (author+) Stored Cross-Site Scripting (XSS) vulnerability in dmitrylitvinov Uploading SVG, WEBP and ICO files plugin <= 1.0.1 at WordPress.	4.8	More Details
CVE-2022-2407	The WP phpMyAdmin WordPress plugin before 5.2.0.4 does not 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-2021-36847	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WebbaPlugins Webba Booking plugin <= 4.2.21 at WordPress.	4.8	More Details
CVE-2022-35117	Clinic's Patient Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via update_medicine_details.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Packing text box under the Update Medical Details module.	4.8	More Details
CVE-2022-0446	The Simple Banner WordPress plugin before 2.12.0 does not properly sanitize its "Simple Banner Text" Settings allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-1322	The Coming Soon - Under Construction WordPress plugin through 1.1.9 does not sanitize and escape some of its settings, which could allow high-privileged users to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2021-36857	Authenticated (editor+) Stored Cross-Site Scripting (XSS) vulnerability in wpshopmart Testimonial Builder plugin <= 1.6.1 at WordPress.	4.8	More Details
CVE-2022-2885	Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.	4.8	More Details
CVE-2022-2789	Emerson Electric's Proficy Machine Edition Version 9.00 and prior is vulnerable to CWE-345 Insufficient Verification of Data Authenticity, and can display logic that is different than the compiled logic.	4.7	More Details
CVE-2022-31238	Dell PowerScale OneFS, versions 9.0.0 up to and including 9.1.0.19, 9.2.1.12, 9.3.0.6, and 9.4.0.2, contain a process invoked with sensitive information vulnerability. A CLI user may potentially exploit this vulnerability, leading to information disclosure.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3521	There is a flaw in RPM's signature functionality. OpenPGP subkeys are associated with a primary key via a "binding signature." RPM does not check the binding signature of subkeys prior to importing them. If an attacker is able to add or socially engineer another party to add a malicious subkey to a legitimate public key, RPM could wrongly trust a malicious signature. The greatest impact of this flaw is to data integrity. To exploit this flaw, an attacker must either compromise an RPM repository or convince an administrator to install an untrusted RPM or public key. It is strongly recommended to only use RPMs and public keys from trusted sources.	4.7	More Details
CVE-2022-34770	Tabit - sensitive information disclosure. Several APIs on the web system display, without authorization, sensitive information such as health statements, previous bills in a specific restaurant, alcohol consumption and smoking habits. Each of the described API's, has in its URL one or more MongoDB ID which is not so simple to enumerate. However, they each receive a 'tiny URL' in Tabit's domain, in the form of https://tbit.be/{suffix} with suffix being a 5 characters long string containing numbers, lower- and upper-case letters. It is not so simple to enumerate them all, but really easy to find some that work and lead to a personal endpoint. This is both an example of OWASP: API4 - rate limiting and OWASP: API1 - Broken object level authorization. Furthermore, the redirect URL disclosed the MongoDB IDs discussed above, and we could use them to query other endpoints disclosing more personal information. For example: The URL https://tabitisrael.co.il/online-reservations/health-statement?orgId={org_id}&healthStatementId={health_statement_id} is used to invite friends to fill a health statement before attending the restaurant. We can use the health_statement_id to access the https://tgm-api.tabit.cloud/health-statement/{health_statement_id} API which disclose medical information as well as id number.	4.6	More Details
CVE-2022-35656	Pega Platform from 8.3 to 8.7.3 vulnerability may allow authenticated security administrators to alter CSRF settings directly.	4.5	More Details
CVE-2021-33128	Improper access control in the firmware for some Intel(R) E810 Ethernet Controllers before version 1.6.0.6 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2022-21240	Out of bounds read for some Intel(R) PROSet/Wireless WiFi products may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33126	Improper access control in the firmware for some Intel(R) 700 and 722 Series Ethernet Controllers and Adapters before versions 8.5 and 1.5.5 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2022-26074	Incomplete cleanup in a firmware subsystem for Intel(R) SPS before versions SPS_E3_04.08.04.330.0 and SPS_E3_04.01.04.530.0 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2022-28709	Improper access control in the firmware for some Intel(R) E810 Ethernet Controllers before version 1.6.1.9 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2022-2965	Improper Restriction of Rendered UI Layers or Frames in GitHub repository notrinos/notrinoserp prior to 0.7.	4.3	More Details
CVE-2022-28882	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure products whereby the aegen.dll will go into an infinite loop when unpacking PE files. This eventually leads to scanning engine crash. The exploit can be triggered remotely by an attacker.	4.3	More Details
CVE-2021-3763	A flaw was found in the Red Hat AMQ Broker management console in version 7.8 where an existing user is able to access some limited information even when the role the user is assigned to should not be allow access to the management console. The main impact is to confidentiality as this flaw means some role bindings are incorrectly checked, some privileged meta information such as queue names and configuration details are disclosed but the impact is limited as not all information is accessible and there is no affect to integrity.	4.3	More Details
CVE-2022-35726	Broken Authentication vulnerability in yotuwp Video Gallery plugin <= 1.3.4.5 at WordPress.	4.3	More Details
CVE-2022-36389	Cross-Site Request Forgery (CSRF) vulnerability in WordPlus Better Messages plugin <= 1.9.9.148 at WordPress.	4.3	More Details
CVE-2021-36852	Cross-Site Request Forgery (CSRF) vulnerability in ThimPress WP Hotel Booking plugin <= 1.10.5 at WordPress.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36346	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in Max Foundry MaxButtons plugin <= 9.2 at WordPress.	4.3	More Details
CVE-2022-33311	Browse restriction bypass vulnerability in Address Book of Cybozu Office 10.0.0 to 10.8.5 allows a remote authenticated attacker to obtain the data of Address Book via unspecified vectors.	4.3	More Details
CVE-2022-2275	The WP Edit Menu WordPress plugin before 1.5.0 does not have CSRF in an AJAX action, which could allow attackers to make a logged in admin delete arbitrary posts/pages from the blog via a CSRF attack	4.3	More Details
CVE-2022-2198	The WPQA Builder WordPress plugin before 5.7 which is a companion plugin to the Hilmer and Discy , does not check authorization before displaying private messages, allowing any logged in user to read other users private message using the message id, which can easily be brute forced.	4.3	More Details
CVE-2022-2382	The Product Slider for WooCommerce WordPress plugin before 2.5.7 has flawed CSRF checks and lack authorisation in some of its AJAX actions, allowing any authenticated users, such as subscriber to call them. One in particular could allow them to delete arbitrary blog options.	4.3	More Details
CVE-2022-2389	The Abandoned Cart Recovery for WooCommerce, Follow Up Emails, Newsletter Builder & Marketing Automation By Autonami WordPress plugin before 2.1.2 does not have authorisation and CSRF checks in one of its AJAX action, allowing any authenticated users, such as subscriber to create automations	4.3	More Details
CVE-2022-32480	Dell PowerScale OneFS, versions 9.0.0, up to and including 9.1.0.19, 9.2.1.12, 9.3.0.6, and 9.4.0.2, contain an insecure default initialization of a resource vulnerability. A remote authenticated attacker may potentially exploit this vulnerability, leading to information disclosure.	4.3	More Details
CVE-2022-2172	The LinkWorth WordPress plugin before 3.3.4 does not implement nonce checks, which could allow attackers to make a logged in admin change settings via a CSRF attack.	4.3	More Details
CVE-2022-1251	The Ask me WordPress theme before 6.8.4 does not perform nonce checks when processing POST requests to the Edit Profile page, allowing an attacker to trick a user to change their profile information by sending a crafted request.	4.3	More Details
CVE-2022-2377	The Directorist WordPress plugin before 7.3.0 does not have authorisation and CSRF checks in an AJAX action, allowing any authenticated users to send arbitrary emails on behalf of the blog	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35204	Vitejs Vite before v2.9.13 was discovered to allow attackers to perform a directory traversal via a crafted URL to the victim's service.	4.3	More Details
CVE-2022-32583	Operation restriction bypass vulnerability in Scheduler of Cybozu Office 10.0.0 to 10.8.5 allows a remote authenticated attacker to alter the data of Scheduler via unspecified vectors.	4.3	More Details
CVE-2022-32544	Operation restriction bypass vulnerability in Project of Cybozu Office 10.0.0 to 10.8.5 allows a remote authenticated attacker to alter the data of Project via unspecified vectors.	4.3	More Details
CVE-2022-34772	Tabit - password enumeration. Description: Tabit - password enumeration. The passwords for the Tabit system is a 4 digit OTP. One can resend OTP and try logging in indefinitely. Once again, this is an example of OWASP: API4 - Rate limiting.	4.3	More Details
CVE-2022-32283	Browse restriction bypass vulnerability in Cabinet of Cybozu Office 10.0.0 to 10.8.5 allows a remote authenticated attacker to obtain the data of Cabinet via unspecified vectors.	4.3	More Details
CVE-2022-29891	Browse restriction bypass vulnerability in Custom Ap of Cybozu Office 10.0.0 to 10.8.5 allows a remote authenticated attacker to obtain the data of Custom App via unspecified vectors.	4.3	More Details
CVE-2022-25986	Browse restriction bypass vulnerability in Scheduler of Cybozu Office 10.0.0 to 10.8.5 allows a remote authenticated attacker to obtain the data of Scheduler.	4.3	More Details
CVE-2022-2276	The WP Edit Menu WordPress plugin before 1.5.0 does not have authorisation and CSRF in an AJAX action, which could allow unauthenticated attackers to delete arbitrary posts/pages from the blog	4.3	More Details
CVE-2022-32768	Multiple authentication bypass vulnerabilities exist in the objects id handling functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request by an authenticated user can lead to unauthorized access and takeover of resources. An attacker can send an HTTP request to trigger this vulnerability.This vulnerability exists in the Live Schedules plugin, allowing an attacker to bypass authentication by guessing a sequential ID, allowing them to take over the another user's streams.	4.2	More Details
CVE-2022-34347	Cross-Site Request Forgery (CSRF) vulnerability in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33900	PHP Object Injection vulnerability in Easy Digital Downloads plugin <= 3.0.1 at WordPress.	4.1	More Details
CVE-2022-2870	A vulnerability was found in laravel 5.1 and classified as problematic. This issue affects some unknown processing. The manipulation leads to deserialization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206501 was assigned to this vulnerability.	4.1	More Details
CVE-2022-2788	Emerson Electric's Proficy Machine Edition Version 9.80 and prior is vulnerable to CWE-29 Path Traversal: '\..\Filename', also known as a ZipSlip attack, through an upload procedure which enables attackers to implant a malicious .BLZ file on the PLC. The file can transfer through the engineering station onto Windows in a way that executes the malicious code.	3.9	More Details
CVE-2022-28883	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure products whereby the aerdl unpack function crashes. This can lead to a possible scanning engine crash. The exploit can be triggered remotely by an attacker.	3.5	More Details
CVE-2022-2956	A vulnerability classified as problematic has been found in ConsoleTVs Noxen. Affected is an unknown function of the file /Noxen-master/users.php. The manipulation of the argument create_user_username with the input "><script>alert(/xss/)</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-207000.	3.5	More Details
CVE-2022-31237	Dell PowerScale OneFS, versions 9.2.0 up to and including 9.2.1.12 and 9.3.0.5 contain an improper preservation of permissions vulnerability in SyncIQ. A low privileged local attacker may potentially exploit this vulnerability, leading to limited information disclosure.	3.3	More Details
CVE-2021-23188	Improper access control for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi products may allow an authenticated user to potentially enable information disclosure via local access.	3.3	More Details
CVE-2020-14394	An infinite loop flaw was found in the USB xHCI controller emulation of QEMU while computing the length of the Transfer Request Block (TRB) Ring. This flaw allows a privileged guest user to hang the QEMU process on the host, resulting in a denial of service.	3.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2841	A vulnerability was found in CrowdStrike Falcon 6.31.14505.0/6.42.15610/6.44.15806. It has been classified as problematic. Affected is an unknown function of the component Uninstallation Handler. The manipulation leads to missing authorization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 6.40.15409, 6.42.15611 and 6.44.15807 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-206880.	2.7	More Details
CVE-2020-27834	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-2020-36257	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-2020-36258	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-2020-35516	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-2020-35515	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-2020-36260	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-2020-36256	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2022-34623	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-32425. Reason: This candidate is a duplicate of CVE-2022-32425. Notes: All CVE users should reference CVE-2022-32425 instead of this candidate.	N/A	More Details
CVE-2020-36259	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36267	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-2020-36261	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-2020-36262	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-23156	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2021-23161	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-2022-35604	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-35601. Reason: This candidate is a duplicate of CVE-2022-35601. Notes: All CVE users should reference CVE-2022-35601 instead of this candidate.	N/A	More Details
CVE-2020-27789	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2021-3724	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-2020-27791	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2021-3771	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-3484	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3408	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-2020-36276	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-2020-36275	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-3894	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-2020-36274	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-2020-36272	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-2020-36271	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-2020-36270	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-2020-36269	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-2020-36268	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-2022-28817	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: No impact could be verified. Notes: none	N/A	More Details
CVE-2020-36266	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36265	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-2020-36264	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-2020-36263	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-2020-36273	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