SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 18 May 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-2022-23660	A remote authentication bypass vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	10.0	More Details
CVE-2022-23658	A remote authentication bypass vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	10.0	More Details
CVE-2022-23657	A remote authentication bypass vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	10.0	More Details
CVE-2021-27446	The Weintek cMT product line is vulnerable to code injection, which may allow an unauthenticated remote attacker to execute commands with root privileges on the operation system.	10.0	More Details
CVE-2022-29316	Complete Online Job Search System v1.0 was discovered to contain a SQL injection vulnerability via /eris/index.php?q=result&searchfor=advancesearch.	9.8	More Details
CVE-2022-29794	The frame scheduling module has a Use After Free (UAF) vulnerability.Successful exploitation of this vulnerability will affect data integrity, availability, and confidentiality.	9.8	More Details
CVE-2022-30413	Covid-19 Travel Pass Management System v1.0 is vulnerable to SQL Injection via /ctpms/classes/Master.php?f=delete_application.	9.8	More Details
CVE-2022-30407	Pharmacy Sales And Inventory System v1.0 is vulnerable to SQL Injection via /pharmacy-sales-and-inventory-system/manage_user.php?id=.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30395	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/classes/Master.php?f=delete_cart.	9.8	More Details
CVE-2022-30392	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/classes/Master.php?f=delete_sub_category.	9.8	More Details
CVE-2022-30391	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/classes/Master.php?f=delete_category.	9.8	More Details
CVE-2022-30387	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/classes/Master.php?f=pay_order.	9.8	More Details
CVE-2022-30386	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/classes/Master.php?f=delete_featured.	9.8	More Details
CVE-2022-30385	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/classes/Master.php?f=delete_order.	9.8	More Details
CVE-2022-30384	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/classes/Master.php?f=delete_inventory.	9.8	More Details
CVE-2022-29383	NETGEAR ProSafe SSL VPN firmware FVS336Gv2 and FVS336Gv3 was discovered to contain a SQL injection vulnerability via USERDBDomains.Domainname at cgi-bin/platform.cgi.	9.8	More Details
CVE-2021-46786	The audio module has a vulnerability in verifying the parameters passed by the application space.Successful exploitation of this vulnerability may cause out-of-bounds memory access.	9.8	More Details
CVE-2022-30370	Air Cargo Management System 1.0 is vulnerable to SQL Injection via /acms/classes/Master.php?f=delete_cargo_type.	9.8	More Details
CVE-2022-22282	SonicWall SMA1000 series firmware 12.4.0, 12.4.1-02965 and earlier versions incorrectly restricts access to a resource using HTTP connections from an unauthorized actor leading to Improper Access Control vulnerability.	9.8	More Details
CVE-2021-42967	Unrestricted file upload in /novel-admin/src/main/java/com/java2nb/common/controller/FileController.java in novel-plus all versions allows allows an attacker to upload malicious JSP files.	9.8	More Details
CVE-2022-29363	Phpok v6.1 was discovered to contain a deserialization vulnerability via the update_f() function in login_control.php. This vulnerability allows attackers to getshell via writing arbitrary files.	9.8	More Details
CVE-2022-29317	Simple Bus Ticket Booking System v1.0 was discovered to contain multiple SQL injection vulnerbilities via the username and password parameters at /assets/partials/_handleLogin.php.	9.8	More Details
CVE-2022-30000	Insurance Management System 1.0 is vulnerable to SQL Injection via /insurance/editPayment.php?recipt_no=.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29999	Insurance Management System 1.0 is vulnerable to SQL Injection via /insurance/editClient.php?client_id=.	9.8	More Details
CVE-2022-29998	Insurance Management System 1.0 is vulnerable to SQL Injection via /insurance/clientStatus.php?client_id=.	9.8	More Details
CVE-2022-29746	Money Transfer Management System 1.0 is vulnerable to SQL Injection via /mtms/classes/Users.php?f=delete.	9.8	More Details
CVE-2022-1715	Account Takeover in GitHub repository neorazorx/facturascripts prior to 2022.07.	9.8	More Details
CVE-2022-30765	Calibre-Web before 0.6.18 allows user table SQL Injection.	9.8	More Details
CVE-2022-28929	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the delid parameter at viewtreatmentrecord.php.	9.8	More Details
CVE-2021-33318	An Input Validation Vulnerability exists in Joel Christner .NET C# packages WatsonWebserver, IpMatcher 1.0.4.1 and below (IpMatcher) and 4.1.3 and below (WatsonWebserver) due to insufficient validation of input IP addresses and netmasks against the internal Matcher list of IP addresses and subnets.	9.8	More Details
CVE-2022-1357	The affected On-Premise cnMaestro allows an unauthenticated attacker to access the cnMaestro server and execute arbitrary code in the privileges of the web server. This lack of validation could allow an attacker to append arbitrary data to the logger command.	9.8	More Details
CVE-2022-30054	In Covid 19 Travel Pass Management 1.0, the code parameter is vulnerable to SQL injection attacks.	9.8	More Details
CVE-2022-30053	In Toll Tax Management System 1.0, the id parameter appears to be vulnerable to SQL injection attacks.	9.8	More Details
CVE-2022-30052	In Home Clean Service System 1.0, the password parameter is vulnerable to SQL injection attacks.	9.8	More Details
CVE-2022-28617	A remote bypass security restrictions vulnerability was discovered in HPE OneView version(s): Prior to 7.0. HPE has provided a software update to resolve this vulnerability in HPE OneView.	9.8	More Details
CVE-2022-24108	The Skyoftech So Listing Tabs module 2.2.0 for OpenCart allows a remote attacker to inject a serialized PHP object via the setting parameter, potentially resulting in the ability to write to files on the server, cause DoS, and achieve remote code execution because of deserialization of untrusted data.	9.8	More Details
CVE-2022-1731	Metasonic Doc WebClient 7.0.14.0 / 7.0.12.0 / 7.0.3.0 is vulnerable to a SQL injection attack in the username field. SSO or System authentication are required to be enabled for vulnerable conditions to exist.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27444	The Weintek cMT product line is vulnerable to various improper access controls, which may allow an unauthenticated attacker to remotely access and download sensitive information and perform administrative actions on behalf of a legitimate administrator.	9.8	More Details
CVE-2022-30055	Prime95 30.7 build 9 suffers from a Buffer Overflow vulnerability that could lead to Remote Code Execution.	9.8	More Details
CVE-2022-1386	The Fusion Builder WordPress plugin before 3.6.2, used in the Avada theme, does not validate a parameter in its forms which could be used to initiate arbitrary HTTP requests. The data returned is then reflected back in the application's response. This could be used to interact with hosts on the server's local network bypassing firewalls and access control measures.	9.8	More Details
CVE-2022-28930	ERP-Pro v3.7.5 was discovered to contain a SQL injection vulnerability via the component /base/SysEveMenuAuthPointMapper.xml..	9.8	More Details
CVE-2022-0867	The Pricing Table WordPress plugin before 3.6.1 fails to properly sanitize and escape user supplied POST data before it is being interpolated in an SQL statement and then executed via an AJAX action available to unauthenticated users	9.8	More Details
CVE-2022-29622	An arbitrary file upload vulnerability in formidable v3.1.4 allows attackers to execute arbitrary code via a crafted filename. NOTE: some third parties dispute this issue because the product has common use cases in which uploading arbitrary files is the desired behavior. Also, there are configuration options in all versions that can change the default behavior of how files are handled. Strapi does not consider this to be a valid vulnerability.	9.8	More Details
CVE-2022-29354	An arbitrary file upload vulnerability in the file upload module of Keystone v4.2.1 allows attackers to execute arbitrary code via a crafted file.	9.8	More Details
CVE-2022-29353	An arbitrary file upload vulnerability in the file upload module of Graphql-upload v13.0.0 allows attackers to execute arbitrary code via a crafted filename.	9.8	More Details
CVE-2022-29351	An arbitrary file upload vulnerability in the file upload module of Tiddlywiki5 v5.2.2 allows attackers to execute arbitrary code via a crafted SVG file. Note: The vendor argues that this is not a legitimate issue and there is no vulnerability here.	9.8	More Details
CVE-2021-42897	A remote command execution (RCE) vulnerability was found in FeMiner wms V1.0 in /wms/src/system/datarec.php. The $_POST[r_name] is directly passed into the $mysqlstr and is executed by exec.	9.8	More Details
CVE-2022-30011	In HMS 1.0 when requesting appointment.php through POST, multiple parameters can lead to a SQL injection vulnerability.	9.8	More Details
CVE-2022-30767	nfs_lookup_reply in net/nfs.c in Das U-Boot through 2022.04 (and through 2022.07-rc2) has an unbounded memcpy with a failed length check, leading to a buffer overflow. NOTE: this issue exists because of an incorrect fix for CVE-2019-14196.	9.8	More Details
CVE-2022-29741	Money Transfer Management System 1.0 is vulnerable to SQL Injection via \mtms\classes\Master.php?f=delete_fee.	9.8	More Details
CVE-2022-29745	Money Transfer Management System 1.0 is vulnerable to SQL Injection via \mtms\classes\Master.php?f=delete_transaction.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30001	Insurance Management System 1.0 is vulnerable to SQL Injection via /insurance/editAgent.php?agent_id=.	9.8	More Details
CVE-2022-29739	Money Transfer Management System 1.0 is vulnerable to SQL Injection via /mtms/admin/?page=user/manage_user&id=.	9.8	More Details
CVE-2022-30063	ftcms <=2.1 was discovered to be vulnerable to code execution attacks .	9.8	More Details
CVE-2022-29748	Simple Client Management System 1.0 is vulnerable to SQL Injection via \cms\admin?page=client/manage_client&id=.	9.8	More Details
CVE-2022-29747	Simple Client Management System 1.0 is vulnerable to SQL Injection via /cms/admin/?page=invoice/manage_invoice&id= // Leak place ---> id.	9.8	More Details
CVE-2022-29539	resi-calltrace in RESI Gemini-Net 4.2 is affected by OS Command Injection. It does not properly check the parameters sent as input before they are processed on the server. Due to the lack of validation of user input, an unauthenticated attacker can bypass the syntax intended by the software (e.g., concatenate `&I;\r\ commands) and inject arbitrary system commands with the privileges of the application user.	9.8	More Details
CVE-2022-30525	A OS command injection vulnerability in the CGI program of Zyxel USG FLEX 100(W) firmware versions 5.00 through 5.21 Patch 1, USG FLEX 200 firmware versions 5.00 through 5.21 Patch 1, USG FLEX 500 firmware versions 5.00 through 5.21 Patch 1, USG FLEX 700 firmware versions 5.00 through 5.21 Patch 1, USG FLEX 50(W) firmware versions 5.10 through 5.21 Patch 1, USG20(W)-VPN firmware versions 5.10 through 5.21 Patch 1, ATP series firmware versions 5.10 through 5.21 Patch 1, VPN series firmware versions 4.60 through 5.21 Patch 1, which could allow an attacker to modify specific files and then execute some OS commands on a vulnerable device.	9.8	More Details
CVE-2022-29738	Money Transfer Management System 1.0 is vulnerable to SQL Injection via /mtms/admin/?page=transaction/send&id=, id.	9.8	More Details
CVE-2022-30592	liblsquic/lsquic_qenc_hdl.c in LiteSpeed QUIC (aka LSQUIC) before 3.1.0 mishandles MAX_TABLE_CAPACITY.	9.8	More Details
CVE-2022-29596	MicroStrategy Enterprise Manager 2022 allows authentication bypass by triggering a login failure and then entering the Uid=/../../../../../../../../../../windows/win.ini%00.jpg&Pwd=_any_password_&ConnMode=1&3054=Login substring for directory traversal.	9.8	More Details
CVE-2022-30450	A Remote Code Execution (RCE) vulnerability exists in waimairen 9.1 via wx.php	9.8	More Details
CVE-2022-30449	Hospital Management System in PHP with Source Code (HMS) 1.0 was discovered to contain a SQL injection vulnerability via the editid parameter in room.php.	9.8	More Details
CVE-2022-30448	Hospital Management System in PHP with Source Code (HMS) 1.0 was discovered to contain a File upload vulnerability in treatmentrecord.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30453	ShopWind <= 3.4.2 has a RCE vulnerability in Database.php	9.8	More Details
CVE-2022-29750	Simple Client Management System 1.0 is vulnerable to SQL Injection via /cms/classes/Master.php?f=delete_service.	9.8	More Details
CVE-2022-30048	Mingsoft MCMS 5.2.7 was discovered to contain a SQL injection vulnerability in /mdiy/dict/list URI via orderBy parameter.	9.8	More Details
CVE-2022-30047	Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability in /mdiy/dict/listExcludeApp URI via orderBy parameter.	9.8	More Details
CVE-2021-34085	Read access violation in the III_dequantize_sample function in mpglibDBL/layer3.c in mp3gain through 1.5.2-r2 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact, a different vulnerability than CVE-2017-9872. CVE-2017-14409, and CVE-2018-10778.	9.8	More Details
CVE-2021-33316	The TRENDnet TI-PG1284i switch(hw v2.0R) prior to version 2.0.2.S0 suffers from an integer underflow vulnerability. This vulnerability exists in its lldp related component. Due to lack of proper validation on length field of ChassisID TLV, by sending a crafted lldp packet to the device, integer underflow would occur and the negative number will be passed to memcpy() later, which may cause buffer overflow or invalid memory access.	9.8	More Details
CVE-2021-33315	The TRENDnet TI-PG1284i switch(hw v2.0R) prior to version 2.0.2.S0 suffers from an integer underflow vulnerability. This vulnerability exists in its lldp related component. Due to lack of proper validation on length field of PortID TLV, by sending a crafted lldp packet to the device, integer underflow would occur and the negative number will be passed to memcpy() later, which may cause buffer overflow or invalid memory access.	9.8	More Details
CVE-2021-38969	IBM Spectrum Virtualize 8.2, 8.3, and 8.4 could allow an attacker to allow unauthorized access due to the reuse of support generated credentials. IBM X-Force ID: 212609.	9.8	More Details
CVE-2022-29009	Multiple SQL injection vulnerabilities via the username and password parameters in the Admin panel of Cyber Cafe Management System Project v1.0 allows attackers to bypass authentication.	9.8	More Details
CVE-2022-29007	Multiple SQL injection vulnerabilities via the username and password parameters in the Admin panel of Dairy Farm Shop Management System v1.0 allows attackers to bypass authentication.	9.8	More Details
CVE-2022-29006	Multiple SQL injection vulnerabilities via the username and password parameters in the Admin panel of Directory Management System v1.0 allows attackers to bypass authentication.	9.8	More Details
CVE-2022-29656	Wedding Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /Wedding-Management/package_detail.php.	9.8	More Details
CVE-2022-29749	Simple Client Management System 1.0 is vulnerable to SQL Injection via /cms/classes/Master.php?f=delete_invoice.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42863	A buffer overflow in ecma_builtin_typedarray_prototype_filter() in JerryScript version fe3a5c0 allows an attacker to construct a fake object or a fake arraybuffer with unlimited size.	9.8	More Details
CVE-2022-29993	Online Sports Complex Booking System 1.0 is vulnerable to SQL Injection via /scbs/admin/bookings/view_booking.php?id=.	9.8	More Details
CVE-2022-29989	Online Sports Complex Booking System 1.0 is vulnerable to SQL Injection via \scbs\classes\Master.php?f=delete_booking.	9.8	More Details
CVE-2022-29307	IonizeCMS v1.0.8.1 was discovered to contain a command injection vulnerability via the function copy_lang_content in application/models/lang_model.php.	9.8	More Details
CVE-2022-29306	IonizeCMS v1.0.8.1 was discovered to contain a SQL injection vulnerability via the id_page parameter in application/models/article_model.php.	9.8	More Details
CVE-2022-29303	SolarView Compact ver.6.00 was discovered to contain a command injection vulnerability via conf_mail.php.	9.8	More Details
CVE-2022-22413	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 223022.	9.8	More Details
CVE-2022-29995	Online Sports Complex Booking System 1.0 is vulnerable to SQL Injection via /scbs/admin/?page=clients/manage_client&id=.	9.8	More Details
CVE-2022-29994	Online Sports Complex Booking System 1.0 is vulnerable to SQL Injection via /scbs/admin/?page=facilities/manage_facility&id=.	9.8	More Details
CVE-2022-29751	Simple Client Management System 1.0 is vulnerable to SQL Injection via /cms/classes/Master.php?f=delete_client.	9.8	More Details
CVE-2022-29992	Online Sports Complex Booking System 1.0 is vulnerable to SQL Injection via /scbs/admin/categories/manage_category.php?id=.	9.8	More Details
CVE-2022-29990	Online Sports Complex Booking System 1.0 is vulnerable to SQL Injection via /scbs/admin/categories/view_category.php?id=.	9.8	More Details
CVE-2022-28616	A remote server-side request forgery (ssrf) vulnerability was discovered in HPE OneView version(s): Prior to 7.0. HPE has provided a software update to resolve this vulnerability in HPE OneView.	9.8	More Details
CVE-2022-29988	Online Sports Complex Booking System 1.0 is vulnerable to SQL Injection via \scbs\classes\Master.php?f=delete.	9.8	More Details
CVE-2022-29987	Online Sports Complex Booking System 1.0 is vulnerable to SQL Injection via /scbs/admin/?page=user/manage_user&id=.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29979	Simple Client Management System 1.0 is vulnerable to SQL Injection via /cms/classes/Master.php?f=delete_designation.	9.8	More Details
CVE-2022-29986	Online Sports Complex Booking System 1.0 is vulnerable to SQL Injection via \scbs\classes\Master.php?f=delete_facility.	9.8	More Details
CVE-2022-29985	Online Sports Complex Booking System 1.0 is vulnerable to SQL Injection via \scbs\classes\Master.php?f=delete_category.	9.8	More Details
CVE-2022-29984	Simple Client Management System 1.0 is vulnerable to SQL Injection via /cms/admin/?page=client/view_client&id=.	9.8	More Details
CVE-2022-29983	Simple Client Management System 1.0 is vulnerable to SQL Injection via /cms/admin/?page=invoice/view_invoice&id=.	9.8	More Details
CVE-2022-29980	Simple Client Management System 1.0 is vulnerable to SQL Injection via /cms/admin/?page=user/manage_user&id=.	9.8	More Details
CVE-2022-29981	Simple Client Management System 1.0 is vulnerable to SQL Injection via /cms/classes/Users.php?f=delete.	9.8	More Details
CVE-2022-29982	Simple Client Management System 1.0 is vulnerable to SQL Injection via /cms/admin/maintenance/manage_service.php?id=.	9.8	More Details
CVE-2021-27442	The Weintek cMT product line is vulnerable to a cross-site scripting vulnerability, which could allow an unauthenticated remote attacker to inject malicious JavaScript code.	9.4	More Details
CVE-2022-25591	BlogEngine.NET v3.3.8.0 was discovered to contain an arbitrary file deletion vulnerability which allows attackers to delete files within the web server root directory via a crafted HTTP request.	9.1	More Details
CVE-2022-1587	An out-of-bounds read vulnerability was discovered in the PCRE2 library in the get_recurse_data_length() function of the pcre2_jit_compile.c file. This issue affects recursions in JIT-compiled regular expressions caused by duplicate data transfers.	9.1	More Details
CVE-2022-29897	On various RAD-ISM-900-EN-* devices by PHOENIX CONTACT an admin user could use the traceroute utility integrated in the WebUI to execute arbitrary code with root privileges on the OS due to an improper input validation in all versions of the firmware.	9.1	More Details
CVE-2022-24856	FlyteConsole is the web user interface for the Flyte platform. FlyteConsole prior to version 0.52.0 is vulnerable to server-side request forgery (SSRF) when FlyteConsole is open to the general internet. An attacker can exploit any user of a vulnerable instance to access the internal metadata server or other unauthenticated URLs. Passing of headers to an unauthorized actor may occur. The patch for this issue deletes the entire `cors_proxy`, as this is not required for console anymore. A patch is available in FlyteConsole version 0.52.0. Disable FlyteConsole availability on the internet as a workaround.	9.1	More Details
CVE-2022-29898	On various RAD-ISM-900-EN-* devices by PHOENIX CONTACT an admin user could use the configuration file uploader in the WebUI to execute arbitrary code with root privileges on the OS due to an improper validation of an integrity check value in all versions of the firmware.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23664	A authenticated remote command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	9.1	More Details
CVE-2022-1586	An out-of-bounds read vulnerability was discovered in the PCRE2 library in the compile_xclass_matchingpath() function of the pcre2_jit_compile.c file. This involves a unicode property matching issue in JIT-compiled regular expressions. The issue occurs because the character was not fully read in case-less matching within JIT.	9.1	More Details
CVE-2022-23666	A authenticated remote command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	9.1	More Details
CVE-2022-23665	A authenticated remote command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	9.1	More Details
CVE-2022-22260	The kernel module has a UAF vulnerability.Successful exploitation of this vulnerability will affect data integrity and availability.	9.1	More Details
CVE-2022-23663	A authenticated remote command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	9.1	More Details
CVE-2022-23662	A authenticated remote command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	9.1	More Details
CVE-2022-23661	A authenticated remote command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	9.1	More Details
CVE-2021-42646	XML External Entity (XXE) vulnerability in the file based service provider creation feature of the Management Console in WSO2 API Manager 2.6.0, 3.0.0, 3.1.0, 3.2.0, and 4.0.0; and WSO2 IS as Key Manager 5.7.0, 5.9.0, and 5.10.0; and WSO2 Identity Server 5.7.0, 5.8.0, 5.9.0, 5.10.0, and 5.11.0. Allows attackers to gain read access to sensitive information or cause a denial of service via crafted GET requests.	9.1	More Details
CVE-2022-1379	URL Restriction Bypass in GitHub repository plantuml/plantuml prior to V1.2022.5. An attacker can abuse this to bypass URL restrictions that are imposed by the different security profiles and achieve server side request forgery (SSRF). This allows accessing restricted internal resources/servers or sending requests to third party servers.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-30958	A cross-site request forgery (CSRF) vulnerability in Jenkins SSH Plugin 2.6.1 and earlier allows attackers to connect to an attacker-specified SSH server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26780	Multiple improper input validation vulnerabilities exists in the libnvram.so nvram_import functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted file can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.An improper input validation vulnerability exists in the `httpd`'s `user_define_init` function. Controlling the `user_define_timeout` nvram variable can lead to remote code execution.	8.8	More Details
CVE-2022-25995	A command execution vulnerability exists in the console inhand functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	8.8	More Details
CVE-2022-30972	A cross-site request forgery (CSRF) vulnerability in Jenkins Storable Configs Plugin 1.0 and earlier allows attackers to have Jenkins parse a local XML file (e.g., archived artifacts) that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery.	8.8	More Details
CVE-2022-30971	Jenkins Storable Configs Plugin 1.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.8	More Details
CVE-2022-30969	A cross-site request forgery (CSRF) vulnerability in Jenkins Autocomplete Parameter Plugin 1.1 and earlier allows attackers to execute arbitrary code without sandbox protection if the victim is an administrator.	8.8	More Details
CVE-2022-30708	Webmin through 1.991, when the Authentic theme is used, allows remote code execution when a user has been manually created (i.e., not created in Virtualmin or Cloudmin). This occurs because settings-editor_write.cgi does not properly restrict the file parameter.	8.8	More Details
CVE-2022-30951	Jenkins WMI Windows Agents Plugin 1.8 and earlier includes the Windows Remote Command library does not implement access control, potentially allowing users to start processes even if they're not allowed to log in.	8.8	More Details
CVE-2022-30950	Jenkins WMI Windows Agents Plugin 1.8 and earlier includes the Windows Remote Command library which has a buffer overflow vulnerability that may allow users able to connect to a named pipe to execute commands on the Windows agent machine.	8.8	More Details
CVE-2021-41965	A SQL injection vulnerability exists in ChurchCRM version 2.0.0 to 4.4.5 that allows an authenticated attacker to issue an arbitrary SQL command to the database through the unsanitized EN_tyid, theID and EID fields used when an Edit action on an existing record is being performed.	8.8	More Details
CVE-2021-42643	cmseasy V7.7.5_20211012 is affected by an arbitrary file write vulnerability. Through this vulnerability, a PHP script file is written to the website server, and accessing this file can lead to a code execution vulnerability.	8.8	More Details
CVE-2022-26042	An OS command injection vulnerability exists in the daretools binary functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	8.8	More Details
CVE-2022-26075	An OS command injection vulnerability exists in the console infactory_wlan functionality of InHand Networks InRouter302 V3.5.37. A specially-crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.	8.8	More Details
CVE-2022-26085	An OS command injection vulnerability exists in the httpd wlscan_ASP functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2022-26420	An OS command injection vulnerability exists in the console infactory_port functionality of InHand Networks InRouter302 V3.5.37. A specially-crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26518	An OS command injection vulnerability exists in the console infactory_net functionality of InHand Networks InRouter302 V3.5.37. A specially-crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.	8.8	More Details
CVE-2022-29611	SAP NetWeaver Application Server for ABAP and ABAP Platform do not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	8.8	More Details
CVE-2022-1182	The Visual Slide Box Builder WordPress plugin through 3.2.9 does not sanitise and escape various parameters before using them in SQL statements via some of its AJAX actions available to any authenticated users (such as subscriber), leading to SQL Injections	8.8	More Details
CVE-2022-1103	The Advanced Uploader WordPress plugin through 4.2 allows any authenticated users like subscriber to upload arbitrary files, such as PHP, which could lead to RCE	8.8	More Details
CVE-2022-26781	Multiple improper input validation vulnerabilities exists in the libnvram.so nvram_import functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted file can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.An improper input validation vulnerability exists in the `httpd`'s `user_define_print` function. Controlling the `user_define_timeout` nvram variable can lead to remote code execution.	8.8	More Details
CVE-2022-21182	A privilege escalation vulnerability exists in the router configuration import functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted HTTP request can lead to increased privileges. An attacker can send an HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2022-26782	Multiple improper input validation vulnerabilities exists in the libnvram.so nvram_import functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted file can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.An improper input validation vulnerability exists in the `httpd`'s `user_define_set_item` function. Controlling the `user_define_timeout` nvram variable can lead to remote code execution.	8.8	More Details
CVE-2021-42651	A Server Side Template Injection (SSTI) vulnerability in Pentest-Collaboration-Framework v1.0.8 allows an authenticated remote attacker to execute arbitrary code through /project/PROJECTNAME/reports/.	8.8	More Details
CVE-2021-42969	Certain Anaconda3 2021.05 are affected by OS command injection. When a user installs Anaconda, an attacker can create a new file and write something in usercustomize.py. When the user opens the terminal or activates Anaconda, the command will be executed.	8.8	More Details
CVE-2022-23139	ZTE's ZXMP M721 product has a permission and access control vulnerability. Since the folder permission viewed by sftp is 666, which is inconsistent with the actual permission. It’s easy for? users to?ignore the modification?of?the file permission configuration, so that low-authority accounts could actually obtain higher operating permissions on key files.	8.8	More Details
CVE-2022-24394	Vulnerability in Fidelis Network and Deception CommandPost enables authenticated command injection through the web interface using the “update_checkfile” value for the “filename” parameter. The vulnerability could allow a specially crafted HTTP request to execute system commands on the CommandPost and return results in an HTTP response via an authenticated session. The vulnerability is present in Fidelis Network and Deception versions prior to 9.4.5. Patches and updates are available to address this vulnerability.	8.8	More Details
CVE-2022-24393	Vulnerability in Fidelis Network and Deception CommandPost enables authenticated command injection through the web interface using the “check_vertica_upgrade” value for the “cpIp” parameter. The vulnerability could allow a specially crafted HTTP request to execute system commands on the CommandPost and return results in an HTTP response via an authenticated session. The vulnerability is present in Fidelis Network and Deception versions prior to 9.4.5. Patches and updates are available to address this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24392	Vulnerability in Fidelis Network and Deception CommandPost enables authenticated command injection through the web interface using the “feed_comm_test” value for the “feed” parameter. The vulnerability could allow a specially crafted HTTP request to execute system commands on the CommandPost and return results in an HTTP response via an authenticated session. The vulnerability is present in Fidelis Network and Deception versions prior to 9.4.5. Patches and updates are available to address this vulnerability.	8.8	More Details
CVE-2022-24391	Vulnerability in Fidelis Network and Deception CommandPost enables SQL injection through the web interface by an attacker with user level access. The vulnerability is present in Fidelis Network and Deception versions prior to 9.4.5. Patches and updates are available to address this vulnerability.	8.8	More Details
CVE-2022-24390	Vulnerability in rconfig “remote_text_file” enables an attacker with user level access to the CLI to inject user level commands into Fidelis Network and Deception CommandPost, Collector, Sensor, and Sandbox components as well as neighboring Fidelis components. The vulnerability is present in Fidelis Network and Deception versions prior to 9.4.5. Patches and updates are available to address this vulnerability.	8.8	More Details
CVE-2022-24389	Vulnerability in rconfig “cert_utils” enables an attacker with user level access to the CLI to inject root level commands into Fidelis Network and Deception CommandPost, Collector, Sensor, and Sandbox components as well as neighboring Fidelis components. The vulnerability is present in Fidelis Network and Deception versions prior to 9.4.5. Patches and updates are available to address this vulnerability.	8.8	More Details
CVE-2022-24388	Vulnerability in rconfig “date” enables an attacker with user level access to the CLI to inject root level commands into Fidelis Network and Deception CommandPost, Collector, Sensor, and Sandbox components as well as neighboring Fidelis components. The vulnerability is present in Fidelis Network and Deception versions prior to 9.4.5. Patches and updates are available to address this vulnerability.	8.8	More Details
CVE-2022-27172	A hard-coded password vulnerability exists in the console infactory functionality of InHand Networks InRouter302 V3.5.37. A specially-crafted network request can lead to privileged operation execution. An attacker can send a sequence of requests to trigger this vulnerability.	8.8	More Details
CVE-2022-30060	ftcms <=2.1 was discovered to be vulnerable to Arbitrary File Write via admin/controllers/tp.php	8.8	More Details
CVE-2022-29429	Remote Code Execution (RCE) in Alexander Stokmann's Code Snippets Extended plugin <= 1.4.7 on WordPress via Cross-Site Request Forgery.	8.8	More Details
CVE-2022-30451	An authenticated user could execute code via a SQLi vulnerability in waimairenCMS before version 9.1.	8.8	More Details
CVE-2022-23669	A remote authorization bypass vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	8.8	More Details
CVE-2022-0573	JFrog Artifactory before 7.36.1 and 6.23.41, is vulnerable to Insecure Deserialization of untrusted data which can lead to DoS, Privilege Escalation and Remote Code Execution when a specially crafted request is sent by a low privileged authenticated user due to insufficient validation of a user-provided serialized object.	8.8	More Details
CVE-2022-29930	SHA1 implementation in JetBrains Ktor Native 2.0.0 was returning the same value. The issue was fixed in Ktor version 2.0.1.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22275	Buffer Overflow vulnerability in B&R Automation Runtime webserver allows an unauthenticated network-based attacker to stop the cyclic program on the device and cause a denial of service.	8.6	More Details
CVE-2022-25762	If a web application sends a WebSocket message concurrently with the WebSocket connection closing when running on Apache Tomcat 8.5.0 to 8.5.75 or Apache Tomcat 9.0.0.M1 to 9.0.20, it is possible that the application will continue to use the socket after it has been closed. The error handling triggered in this case could cause the a pooled object to be placed in the pool twice. This could result in subsequent connections using the same object concurrently which could result in data being returned to the wrong use and/or other errors.	8.6	More Details
CVE-2022-1118	Connected Components Workbench (v13.00.00 and prior), ISaGRAF Workbench (v6.0 though v6.6.9), and Safety Instrumented System Workstation (v1.2 and prior (for Trusted Controllers)) do not limit the objects that can be deserialized. This allows attackers to craft a malicious serialized object that, if opened by a local user in Connected Components Workbench, may result in arbitrary code execution. This vulnerability requires user interaction to be successfully exploited	8.6	More Details
CVE-2022-30945	Jenkins Pipeline: Groovy Plugin 2689.v434009a_31b_f1 and earlier allows loading any Groovy source files on the classpath of Jenkins and Jenkins plugins in sandboxed pipelines.	8.5	More Details
CVE-2022-28181	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where an unprivileged regular user on the network can cause an out-of-bounds write through a specially crafted shader, which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering. The scope of the impact may extend to other components.	8.5	More Details
CVE-2022-28182	NVIDIA GPU Display Driver for Windows contains a vulnerability in the DirectX11 user mode driver (nvwgf2um/x.dll), where an unauthorized attacker on the network can cause an out-of-bounds write through a specially crafted shader, which may lead to code execution to cause denial of service, escalation of privileges, information disclosure, and data tampering. The scope of the impact may extend to other components.	8.5	More Details
CVE-2021-43066	A external control of file name or path in Fortinet FortiClientWindows version 7.0.2 and below, version 6.4.6 and below, version 6.2.9 and below, version 6.0.10 and below allows attacker to escalate privilege via the MSI installer.	8.4	More Details
CVE-2022-24831	OpenClinica is an open source software for Electronic Data Capture (EDC) and Clinical Data Management (CDM). Versions prior to 3.16.1 are vulnerable to SQL injection due to the use of string concatenation to create SQL queries instead of prepared statements. No known workarounds exist. This issue has been patched in 3.16.1, 3.15.9, 3.14.1, and 3.13.1 and users are advised to upgrade.	8.3	More Details
CVE-2021-27771	User SID can be modified resulting in an Arbitrary File Upload or deletion of directories causing a Denial of Service. When interacting in a normal matter with the Sametime chat application, users hold a cookie containing their session ID (SID). This value is also used when sending chat messages, receiving notifications and/or transferring files.	8.2	More Details
CVE-2021-27478	A specifically crafted packet sent by an attacker to EIPStackGroup OpENer EtherNet/IP commits and versions prior to Feb 10, 2021 may cause a denial-of-service condition.	8.2	More Details
CVE-2022-1360	The affected On-Premise cnMaestro is vulnerable to execution of code on the cnMaestro hosting server. This could allow a remote attacker to change server configuration settings.	8.2	More Details
CVE-2021-33013	mySCADA myPRO versions prior to 8.20.0 does not restrict unauthorized read access to sensitive system information.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21809	A file write vulnerability exists in the httpd upload.cgi functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted HTTP request can lead to arbitrary file upload. An attacker can upload a malicious file to trigger this vulnerability.	8.1	More Details
CVE-2022-1650	Improper Removal of Sensitive Information Before Storage or Transfer in GitHub repository eventsource/eventsource prior to v2.0.2.	8.1	More Details
CVE-2022-29174	countly-server is the server-side part of Countly, a product analytics solution. Prior to versions 22.03.7 and 21.11.4, a malicious actor who knows an account email address/username and full name specified in the database is capable of guessing the password reset token. The actor may use this information to reset the password and take over the account. The problem has been patched in Countly Server version 22.03.7 for servers using the new user interface and in 21.11.4 for servers using the old user interface.	8.1	More Details
CVE-2020-22983	A Server-Side Request Forgery (SSRF) vulnerability exists in MicroStrategy Web SDK 11.1 and earlier, allows remote unauthenticated attackers to conduct a server-side request forgery (SSRF) attack via the srcURL parameter to the shortURL task.	8.1	More Details
CVE-2022-25865	The package workspace-tools before 0.18.4 are vulnerable to Command Injection via git argument injection. When calling the fetchRemoteBranch(remote: string, remoteBranch: string, cwd: string) function, both the remote and remoteBranch parameters are passed to the git fetch subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection.	8.1	More Details
CVE-2022-22775	The Workspace client component of TIBCO Software Inc.'s TIBCO BPM Enterprise and TIBCO BPM Enterprise Distribution for TIBCO Silver Fabric contains difficult to exploit Reflected Cross Site Scripting (XSS) vulnerabilities that allow low privileged attackers with network access to execute scripts targeting the affected system or the victim's local system. Affected releases are TIBCO Software Inc.'s TIBCO BPM Enterprise: versions 4.3.1 and below and TIBCO BPM Enterprise Distribution for TIBCO Silver Fabric: versions 4.3.1 and below.	8.1	More Details
CVE-2021-0126	Improper input validation for the Intel(R) Manageability Commander before version 2.2 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	8.0	More Details
CVE-2022-30594	The Linux kernel before 5.17.2 mishandles seccomp permissions. The PTRACE_SEIZE code path allows attackers to bypass intended restrictions on setting the PT_SUSPEND_SECCOMP flag.	7.8	More Details
CVE-2021-0189	Use of out-of-range pointer offset in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable aescalation of privilege via local access.	7.8	More Details
CVE-2021-0188	Return of pointer value outside of expected range in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable aescalation of privilege via local access.	7.8	More Details
CVE-2021-0159	Improper input validation in the BIOS authenticated code module for some Intel(R) Processors may allow a privileged user to potentially enable aescalation of privilege via local access.	7.8	More Details
CVE-2021-0154	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable aescalation of privilege via local access.	7.8	More Details
CVE-2021-0153	Out-of-bounds write in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable aescalation of privilege via local access.	7.8	More Details
CVE-2022-29581	Improper Update of Reference Count vulnerability in net/sched of Linux Kernel allows local attacker to cause privilege escalation to root. This issue affects: Linux Kernel versions prior to 5.18; version 4.14 and later versions.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1735	Classic Buffer Overflow in GitHub repository vim/vim prior to 8.2.4969.	7.8	More Details
CVE-2021-26258	Improper access control for the Intel(R) Killer(TM) Control Center software before version 2.4.3337.0 may allow an authorized user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-30688	needrestart 0.8 through 3.5 before 3.6 is prone to local privilege escalation. Regexes to detect the Perl, Python, and Ruby interpreters are not anchored, allowing a local user to escalate privileges when needrestart tries to detect if interpreters are using old source files.	7.8	More Details
CVE-2022-28838	Acrobat Acrobat Pro DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by a use-after-free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-28243	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-28242	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by a use-after-free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-28241	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-28240	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by a use-after-free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-28239	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-0190	Uncaught exception in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable aescalation of privilege via local access.	7.8	More Details
CVE-2021-33122	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable aescalation of privilege via local access.	7.8	More Details
CVE-2022-28826	Adobe Framemaker versions 2029u8 (and earlier) and 2020u4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-1679	A use-after-free flaw was found in the Linux kernel's Atheros wireless adapter driver in the way a user forces the ath9k_htc_wait_for_target function to fail with some input messages. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26386	A malicious or compromised UApp or ABL may be used by an attacker to issue a malformed system call to the Stage 2 Bootloader potentially leading to corrupt memory and code execution.	7.8	More Details
CVE-2021-26317	Failure to verify the protocol in SMM may allow an attacker to control the protocol and modify SPI flash resulting in a potential arbitrary code execution.	7.8	More Details
CVE-2021-26369	A malicious or compromised UApp or ABL may be used by an attacker to send a malformed system call to the bootloader, resulting in out-of-bounds memory accesses.	7.8	More Details
CVE-2022-28234	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) is affected by a heap-based buffer overflow vulnerability due to insecure handling of a crafted .pdf file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file	7.8	More Details
CVE-2022-22281	A buffer overflow vulnerability in the SonicWall SSL-VPN NetExtender Windows Client (32 and 64 bit) in 10.2.322 and earlier versions, allows an attacker to potentially execute arbitrary code in the host windows operating system.	7.8	More Details
CVE-2022-29623	An arbitrary file upload vulnerability in the file upload module of Connect-Multiparty v2.2.0 allows attackers to execute arbitrary code via a crafted PDF file.	7.8	More Details
CVE-2022-30523	Trend Micro Password Manager (Consumer) version 5.0.0.1266 and below is vulnerable to a Link Following Privilege Escalation Vulnerability that could allow a low privileged local attacker to delete the contents of an arbitrary folder as SYSTEM which can then be used for privilege escalation on the affected machine.	7.8	More Details
CVE-2022-30695	Local privilege escalation due to excessive permissions assigned to child processes. The following products are affected: Acronis Snap Deploy (Windows) before build 3640	7.8	More Details
CVE-2021-33123	Improper access control in the BIOS authenticated code module for some Intel(R) Processors may allow a privileged user to potentially enable aescalation of privilege via local access.	7.8	More Details
CVE-2022-30696	Local privilege escalation due to a DLL hijacking vulnerability. The following products are affected: Acronis Snap Deploy (Windows) before build 3640	7.8	More Details
CVE-2022-30697	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Snap Deploy (Windows) before build 3640	7.8	More Details
CVE-2022-1116	Integer Overflow or Wraparound vulnerability in io_uring of Linux Kernel allows local attacker to cause memory corruption and escalate privileges to root. This issue affects: Linux Kernel versions prior to 5.4.189; version 5.4.24 and later versions.	7.8	More Details
CVE-2022-1733	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.4968.	7.8	More Details
CVE-2022-1769	Buffer Over-read in GitHub repository vim/vim prior to 8.2.4974.	7.8	More Details
CVE-2022-21128	Insufficient control flow management in the Intel(R) Advisor software before version 7.6.0.37 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40399	An exploitable use-after-free vulnerability exists in WPS Spreadsheets (ET) as part of WPS Office, version 11.2.0.10351. A specially-crafted XLS file can cause a use-after-free condition, resulting in remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	7.8	More Details
CVE-2022-28236	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-23742	Check Point Endpoint Security Client for Windows versions earlier than E86.40 copy files for forensics reports from a directory with low privileges. An attacker can replace those files with malicious or linked content, such as exploiting CVE-2020-0896 on unpatched systems or using symbolic links.	7.8	More Details
CVE-2022-28214	During an update of SAP BusinessObjects Enterprise, Central Management Server (CMS) - versions 420, 430, authentication credentials are being exposed in Sysmon event logs. This Information Disclosure could cause a high impact on systems' Confidentiality, Integrity, and Availability.	7.8	More Details
CVE-2022-24102	Acrobat Reader DC versions 20.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-23743	Check Point ZoneAlarm before version 15.8.200.19118 allows a local actor to escalate privileges during the upgrade process. In addition, weak permissions in the ProgramData\CheckPoint\ZoneAlarm\Data\Updates directory allow a local attacker the ability to execute an arbitrary file write, leading to execution of code as local system, in ZoneAlarm versions before v15.8.211.192119	7.8	More Details
CVE-2022-27794	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) is affected by the use of a variable that has not been initialized when processing of embedded fonts, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file	7.8	More Details
CVE-2022-29218	RubyGems is a package registry used to supply software for the Ruby language ecosystem. An ordering mistake in the code that accepts gem uploads allowed some gems (with platforms ending in numbers, like `arm64-darwin-21`) to be temporarily replaced in the CDN cache by a malicious package. The bug has been patched, and is believed to have never been exploited, based on an extensive review of logs and existing gems by rubygems. The easiest way to ensure that an application has not been exploited by this vulnerability is to verify all downloaded .gems checksums match the checksum recorded in the RubyGems.org database. RubyGems.org has been patched and is no longer vulnerable to this issue.	7.7	More Details
CVE-2022-28183	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where an unprivileged regular user can cause an out-of-bounds read, which may lead to denial of service and information disclosure.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22773	The REST API component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server - Community Edition, TIBCO JasperReports Server - Developer Edition, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for ActiveMatrix BPM, and TIBCO JasperReports Server for Microsoft Azure contains difficult to exploit Reflected Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker with network access to execute scripts targeting the affected system or the victim's local system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions 8.0.1 and below, TIBCO JasperReports Server - Community Edition: versions 8.0.1 and below, TIBCO JasperReports Server - Developer Edition: versions 8.0.0 and below, TIBCO JasperReports Server for AWS Marketplace: versions 8.0.1 and below, TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.9.2 and below, and TIBCO JasperReports Server for Microsoft Azure: versions 8.0.1 and below.	7.7	More Details
CVE-2021-23267	Improper Control of Dynamically-Managed Code Resources vulnerability in Crafter Studio of Crafter CMS allows authenticated developers to execute OS commands via FreeMarker static methods.	7.6	More Details
CVE-2022-22252	The DFX module has a UAF vulnerability.Successful exploitation of this vulnerability may affect system stability.	7.5	More Details
CVE-2022-30040	Tenda AX1803 v1.0.0.1_2890 is vulnerable to Buffer Overflow. The vulnerability lies in rootfs_ In / goform / setsystimecfg of / bin / tdhttpd in ubif file system, attackers can access http://ip/goform/SetSysTimeCfg, and by setting the ntpserve parameter, the stack buffer overflow can be caused to achieve the effect of router denial of service.	7.5	More Details
CVE-2022-1701	SonicWall SMA1000 series firmware 12.4.0, 12.4.1-02965 and earlier versions uses a shared and hard-coded encryption key to store data.	7.5	More Details
CVE-2022-29847	In Progress Ipswitch WhatsUp Gold 21.0.0 through 21.1.1, and 22.0.0, it is possible for an unauthenticated attacker to invoke an API transaction that would allow them to relay encrypted WhatsUp Gold user credentials to an arbitrary host.	7.5	More Details
CVE-2021-33005	mySCADA myPRO versions prior to 8.20.0 allows an unauthenticated remote attacker to upload arbitrary files to arbitrary directories.	7.5	More Details
CVE-2022-21190	This affects the package convict before 6.2.3. This is a bypass of [CVE-2022-22143] (https://security.snyk.io/vuln/SNYK-JS-CONVICT-2340604). The [fix] (https://github.com/mozilla/node-convict/commit/3b86be087d8f14681a9c889d45da7fe3ad9cd880) introduced, relies on the startsWith method and does not prevent the vulnerability: before splitting the path, it checks if it starts with __proto__ or this.constructor.prototype. To bypass this check it's possible to prepend the dangerous paths with any string value followed by a dot, like for example foo.__proto__ or foo.this.constructor.prototype.	7.5	More Details
CVE-2022-29616	SAP Host Agent, SAP NetWeaver and ABAP Platform allow an attacker to leverage logical errors in memory management to cause a memory corruption.	7.5	More Details
CVE-2022-28936	FISCO-BCOS release-3.0.0-rc2 was discovered to contain an issue where a malicious node can trigger an integer overflow and cause a Denial of Service (DoS) via an unusually large viewchange message packet.	7.5	More Details
CVE-2022-28937	FISCO-BCOS release-3.0.0-rc2 was discovered to contain an issue where a malicious node, via an invalid proposal with an invalid header, will cause normal nodes to stop producing new blocks and processing new clients' requests.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30049	A Server-Side Request Forgery (SSRF) in Rebuild v2.8.3 allows attackers to obtain the real IP address and scan Intranet information via the fileurl parameter.	7.5	More Details
CVE-2021-33009	mySCADA myPRO versions prior to 8.20.0 allows an unauthenticated remote attacker to upload arbitrary files to the file system.	7.5	More Details
CVE-2022-29796	The HiAIserver has a vulnerability in verifying the validity of the weight used in the model.Successful exploitation of this vulnerability will affect AI services.	7.5	More Details
CVE-2021-27505	mySCADA myPRO versions prior to 8.20.0 does not restrict unauthorized read access to sensitive directory listing information.	7.5	More Details
CVE-2022-30781	Gitea before 1.16.7 does not escape git fetch remote.	7.5	More Details
CVE-2022-22261	The HiAIserver has a vulnerability in verifying the validity of the weight used in the model.Successful exploitation of this vulnerability will affect AI services.	7.5	More Details
CVE-2022-29789	The HiAIserver has a vulnerability in verifying the validity of the properties used in the model.Successful exploitation of this vulnerability will affect AI services.	7.5	More Details
CVE-2022-29298	SolarView Compact ver.6.00 allows attackers to access sensitive files via directory traversal.	7.5	More Details
CVE-2022-30557	Foxit PDF Reader and PDF Editor before 11.2.2 have a Type Confusion issue that causes a crash because of Unsigned32 mishandling during JavaScript execution.	7.5	More Details
CVE-2022-29790	The graphics acceleration service has a vulnerability in multi-thread access to the database.Successful exploitation of this vulnerability may cause service exceptions.	7.5	More Details
CVE-2022-29791	The HiAIserver has a vulnerability in verifying the validity of the weight used in the model.Successful exploitation of this vulnerability will affect AI services.	7.5	More Details
CVE-2022-1699	Uncontrolled Resource Consumption in GitHub repository causefx/organizr prior to 2.1.2000. This vulnerability can be abused by doing a DDoS attack for which genuine users will not able to access resources/applications.	7.5	More Details
CVE-2022-29885	The documentation of Apache Tomcat 10.1.0-M1 to 10.1.0-M14, 10.0.0-M1 to 10.0.20, 9.0.13 to 9.0.62 and 8.5.38 to 8.5.78 for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks.	7.5	More Details
CVE-2022-1698	Allowing long password leads to denial of service in GitHub repository causefx/organizr prior to 2.1.2000. This vulnerability can be abused by doing a DDoS attack for which genuine users will not able to access resources/applications.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30279	An issue was discovered in Stormshield Network Security (SNS) 4.3.x before 4.3.8. The event logging of the ASQ sofbus lacbus plugin triggers the dereferencing of a NULL pointer, leading to a crash of SNS. An attacker could exploit this vulnerability via forged sofbus lacbus traffic to cause a firmware crash.	7.5	More Details
CVE-2022-29792	The chip component has a vulnerability of disclosing CPU SNs.Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-30763	Janet before 1.22.0 mishandles arrays.	7.5	More Details
CVE-2022-30782	Openmoney API through 2020-06-29 uses the JavaScript Math.random function, which does not provide cryptographically secure random numbers.	7.5	More Details
CVE-2022-30948	Jenkins Mercurial Plugin 2.16 and earlier allows attackers able to configure pipelines to check out some SCM repositories stored on the Jenkins controller's file system using local paths as SCM URLs, obtaining limited information about other projects' SCM contents.	7.5	More Details
CVE-2022-29588	Konica Minolta bizhub MFP devices before 2022-04-14 use cleartext password storage for the /var/log/nginx/html/ADMINPASS and /etc/shadow files.	7.5	More Details
CVE-2021-3254	Asus DSL-N14U-B1 1.1.2.3_805 allows remote attackers to cause a Denial of Service (DoS) via a TCP SYN scan using nmap.	7.5	More Details
CVE-2021-33317	The TRENDnet TI-PG1284i switch(hw v2.0R) prior to version 2.0.2.S0 suffers from a null pointer dereference vulnerability. This vulnerability exists in its lldp related component. Due to fail to check if ChassisID TLV is contained in the packet, by sending a crafted lldp packet to the device, an attacker can crash the process due to null pointer dereference.	7.5	More Details
CVE-2022-29369	Nginx NJS v0.7.2 was discovered to contain a segmentation violation via njs_lvlhsh_bucket_find at njs_lvlhsh.c.	7.5	More Details
CVE-2022-29932	The HTTP Server in PRIMEUR SPAZIO 2.5.1.954 (File Transfer) allows an unauthenticated attacker to obtain sensitive data (related to the content of transferred files) via a crafted HTTP request.	7.5	More Details
CVE-2021-27482	A specifically crafted packet sent by an attacker to EIPStackGroup OpENer EtherNet/IP commits and versions prior to Feb 10, 2021 may allow the attacker to read arbitrary data.	7.5	More Details
CVE-2021-27498	A specifically crafted packet sent by an attacker to EIPStackGroup OpENer EtherNet/IP commits and versions prior to Feb 10, 2021 may result in a denial-of-service condition.	7.5	More Details
CVE-2021-27500	A specifically crafted packet sent by an attacker to EIPStackGroup OpENer EtherNet/IP commits and versions prior to Feb 10, 2021 may result in a denial-of-service condition.	7.5	More Details
CVE-2022-23671	A remote authenticated information disclosure vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27777	XML External Entity (XXE) injection vulnerabilities occur when poorly configured XML parsers process user supplied input without sufficient validation. Attackers can exploit this vulnerability to manipulate XML content and inject malicious external entity references.	7.5	More Details
CVE-2022-27134	EOSIO batdappboomx v327c04cf has an Access-control vulnerability in the `transfer` function of the smart contract which allows remote attackers to win the cryptocurrency without paying ticket fee via the `std::string memo` parameter.	7.5	More Details
CVE-2021-38872	IBM DataPower Gateway 10.0.2.0, 10.0.3.0, 10.0.1.0 through 10.0.1.4, and 2018.4.1.0 through 2018.4.1.17 could allow a remote user to cause a denial of service by consuming resources with multiple requests. IBM X-Force ID: 208348.	7.5	More Details
CVE-2020-4994	IBM DataPower Gateway 10.0.1.0 through 10.0.1.4 and 2018.4.1.0 through 2018.4.1.17 could allow a remote user to cause a temporary denial of service by sending invalid HTTP requests. IBM X-Force ID: 192906.	7.5	More Details
CVE-2022-29793	There is a configuration defect in the activation lock of mobile phones.Successful exploitation of this vulnerability may affect application availability.	7.5	More Details
CVE-2022-30947	Jenkins Git Plugin 4.11.1 and earlier allows attackers able to configure pipelines to check out some SCM repositories stored on the Jenkins controller's file system using local paths as SCM URLs, obtaining limited information about other projects' SCM contents.	7.5	More Details
CVE-2022-1711	Server-Side Request Forgery (SSRF) in GitHub repository jgraph/drawio prior to 18.0.5.	7.5	More Details
CVE-2022-1723	Server-Side Request Forgery (SSRF) in GitHub repository jgraph/drawio prior to 18.0.6.	7.5	More Details
CVE-2022-26650	In Apache ShenYui, ShenYu-Bootstrap, RegexPredicateJudge.java uses Pattern.matches(conditionData.getParamValue(), realData) to make judgments, where both parameters are controllable by the user. This can cause an attacker pass in malicious regular expressions and characters causing a resource exhaustion. This issue affects Apache ShenYu (incubating) 2.4.0, 2.4.1 and 2.4.2 and is fixed in 2.4.3.	7.5	More Details
CVE-2021-46787	The AMS module has a vulnerability of improper permission control.Successful exploitation of this vulnerability may cause non-system application processes to crash.	7.5	More Details
CVE-2022-1721	Path Traversal in WellKnownServlet in GitHub repository jgraph/drawio prior to 18.0.5. Read local files of the web application.	7.5	More Details
CVE-2022-1713	SSRF on /proxy in GitHub repository jgraph/drawio prior to 18.0.4. An attacker can make a request as the server and read its contents. This can lead to a leak of sensitive information.	7.5	More Details
CVE-2021-46788	Third-party pop-up window coverage vulnerability in the iConnect module.Successful exploitation of this vulnerability may cause system pop-up window may be covered to mislead users to perform incorrect operations.	7.5	More Details
CVE-2021-46789	Configuration defects in the secure OS module. Successful exploitation of this vulnerability can affect availability.	7.5	More Details
CVE-2021-42870	ACCEL-PPP 1.12.0 has an out-of-bounds read in post_msg when processing a call_clear_request.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30012	In the POST request of the appointment.php page of HMS v.0, there are SQL injection vulnerabilities in multiple parameters, and database information can be obtained through injection.	7.5	More Details
CVE-2022-29795	The frame scheduling module has a null pointer dereference vulnerability. Successful exploitation of this vulnerability will affect the kernel availability.	7.5	More Details
CVE-2022-1361	The affected On-Premise cnMaestro is vulnerable to a pre-auth data exfiltration through improper neutralization of special elements used in an SQL command. This could allow an attacker to exfiltrate data about other user's accounts and devices.	7.4	More Details
CVE-2022-29586	Konica Minolta bizhub MFP devices before 2022-04-14 allow a Sandbox Escape. An attacker must attach a keyboard to a USB port, press F12, and then escape from the kiosk mode.	7.4	More Details
CVE-2022-22139	Uncontrolled search path in the Intel(R) XTU software before version 7.3.0.33 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.3	More Details
CVE-2021-37851	Local privilege escalation in Windows products of ESET allows user who is logged into the system to exploit repair feature of the installer to run malicious code with higher privileges. This issue affects: ESET, spol. s r.o. ESET NOD32 Antivirus 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Internet Security 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Smart Security Premium 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Endpoint Antivirus 6.0 versions prior to 9.0.2046.0; 6.0 versions prior to 8.1.2050.0; 6.0 versions prior to 8.0.2053.0. ESET, spol. s r.o. ESET Endpoint Security 6.0 versions prior to 9.0.2046.0; 6.0 versions prior to 8.1.2050.0; 6.0 versions prior to 8.0.2053.0. ESET, spol. s r.o. ESET Server Security for Microsoft Windows Server 8.0 versions prior to 9.0.12012.0. ESET, spol. s r.o. ESET File Security for Microsoft Windows Server 8.0.12013.0. ESET, spol. s r.o. ESET Mail Security for Microsoft Exchange Server 6.0 versions prior to 8.0.10020.0. ESET, spol. s r.o. ESET Mail Security for IBM Domino 6.0 versions prior to 8.0.14011.0. ESET, spol. s r.o. ESET Security for Microsoft SharePoint Server 6.0 versions prior to 8.0.15009.0.	7.3	More Details
CVE-2021-34605	A zip slip vulnerability in XINJE XD/E Series PLC Program Tool up to version v3.5.1 can provide an attacker with arbitrary file write privilege when opening a specially-crafted project file. This vulnerability can be triggered by manually opening an infected project file, or by initiating an upload program request from an infected Xinje PLC. This can result in remote code execution, information disclosure and denial of service of the system running the XINJE XD/E Series PLC Program Tool.	7.3	More Details
CVE-2021-34606	A vulnerability exists in XINJE XD/E Series PLC Program Tool in versions up to v3.5.1 that can allow an authenticated, local attacker to load a malicious DLL. Local access is required to successfully exploit this vulnerability. This means the potential attacker must have access to the system and sufficient file-write privileges. If exploited, the attacker could place a malicious DLL file on the system, that when running XINJE XD/E Series PLC Program Tool will allow the attacker to execute arbitrary code with the privileges of another user's account.	7.3	More Details
CVE-2022-30396	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/admin/?page=inventory/manage_inventory&id=.	7.2	More Details
CVE-2020-19228	An issue was found in bludit v3.13.0, unsafe implementation of the backup plugin allows attackers to upload arbitrary files.	7.2	More Details
CVE-2022-30373	Air Cargo Management System 1.0 is vulnerable to SQL Injection via /acms/admin/cargo_types/manage_cargo_type.php?id=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30372	Air Cargo Management System 1.0 is vulnerable to SQL Injection via /acms/classes/Master.php?f=delete_cargo.	7.2	More Details
CVE-2022-30371	Air Cargo Management System 1.0 is vulnerable to SQL Injection via /acms/admin/cargo_types/view_cargo_type.php?id=.	7.2	More Details
CVE-2022-30007	GXCMS V1.5 has a file upload vulnerability in the background. The vulnerability is the template management page. You can edit any template content and then rename to PHP suffix file, after calling PHP file can control the server.	7.2	More Details
CVE-2022-23672	A authenticated remote command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2022-30393	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/admin/?page=product/manage_product&id=.	7.2	More Details
CVE-2022-23673	A authenticated remote command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2022-29655	An arbitrary file upload vulnerability in the Upload Photos module of Wedding Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-0024	A vulnerability exists in Palo Alto Networks PAN-OS software that enables an authenticated network-based PAN-OS administrator to upload a specifically created configuration that disrupts system processes and potentially execute arbitrary code with root privileges when the configuration is committed on both hardware and virtual firewalls. This issue does not impact Panorama appliances or Prisma Access customers. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.23; PAN-OS 9.0 versions earlier than PAN-OS 9.0.16; PAN-OS 9.1 versions earlier than PAN-OS 9.1.13; PAN-OS 10.0 versions earlier than PAN-OS 10.0.10; PAN-OS 10.1 versions earlier than PAN-OS 10.1.5.	7.2	More Details
CVE-2022-26007	An OS command injection vulnerability exists in the console factory functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted network request can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2022-26002	A stack-based buffer overflow vulnerability exists in the console factory functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted network request can lead to remote code execution. An attacker can send a sequence of malicious packets to trigger this vulnerability.	7.2	More Details
CVE-2022-29318	An arbitrary file upload vulnerability in the New Entry module of Car Rental Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-30374	Air Cargo Management System 1.0 is vulnerable to SQL Injection via /acms/admin/?page=transactions/manage_transaction&id=.	7.2	More Details
CVE-2022-30376	Sourcecodester Simple Social Networking Site v1.0 is vulnerable to SQL Injection via /sns/admin/members/view_member.php?id=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30378	Sourcecodester Simple Social Networking Site v1.0 is vulnerable to SQL Injection via /sns/admin/?page=posts/view_post&id=.	7.2	More Details
CVE-2022-30404	College Management System v1.0 is vulnerable to SQL Injection via /College_Management_System/admin/display-teacher.php?teacher_id=.	7.2	More Details
CVE-2022-30398	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/admin/?page=orders/view_order&id=.	7.2	More Details
CVE-2022-30399	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/admin/?page=maintenance/manage_category&id=.	7.2	More Details
CVE-2022-30400	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/admin/orders/view_order.php?view=user&id=.	7.2	More Details
CVE-2022-30401	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/?p=view_product&id=.	7.2	More Details
CVE-2022-30402	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/admin/?page=maintenance/manage_sub_category&id=.	7.2	More Details
CVE-2022-30403	Merchandise Online Store v1.0 is vulnerable to SQL Injection via /vloggers_merch/?p=products&c=.	7.2	More Details
CVE-2022-30411	Covid-19 Travel Pass Management System v1.0 is vulnerable to SQL Injection via /ctpms/admin/?page=individuals/view_individual&id=.	7.2	More Details
CVE-2022-30379	Sourcecodester Simple Social Networking Site v1.0 is vulnerable to SQL Injection via /sns/admin/?page=user/manage_user&id=.	7.2	More Details
CVE-2022-30412	Covid-19 Travel Pass Management System v1.0 is vulnerable to SQL Injection via /ctpms/admin/individuals/update_status.php?id=.	7.2	More Details
CVE-2022-30414	Covid-19 Travel Pass Management System v1.0 is vulnerable to SQL Injection via /ctpms/admin/?page=applications/view_application&id=.	7.2	More Details
CVE-2022-30415	Covid-19 Travel Pass Management System v1.0 is vulnerable to SQL Injection via /ctpms/admin/applications/update_status.php?id=.	7.2	More Details
CVE-2021-25119	The AGIL WordPress plugin through 1.0 accepts all zip files and automatically extracts the zip file without validating the extracted file type. Allowing high privilege users such as admin to upload an arbitrary file like PHP, leading to RCE	7.2	More Details
CVE-2022-1409	The VikBooking Hotel Booking Engine & PMS WordPress plugin before 1.5.8 does not properly validate images, allowing high privilege users such as administrators to upload PHP files disguised as images and containing malicious PHP code	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23667	A authenticated remote command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	7.2	More Details
CVE-2022-30417	Covid-19 Travel Pass Management System v1.0 is vulnerable to SQL Injection via ctpms/admin/?page=user/manage_user&id=.	7.2	More Details
CVE-2022-26116	Multiple improper neutralization of special elements used in SQL commands ('SQL Injection') vulnerability [CWE-89] in FortiNAC version 8.3.7 and below, 8.5.2 and below, 8.5.4, 8.6.0, 8.6.5 and below, 8.7.6 and below, 8.8.11 and below, 9.1.5 and below, 9.2.2 and below may allow an authenticated attacker to execute unauthorized code or commands via specifically crafted strings parameters.	7.2	More Details
CVE-2021-0193	Improper authentication in the Intel(R) In-Band Manageability software before version 2.13.0 may allow a privileged user to potentially enable escalation of privilege via network access.	7.2	More Details
CVE-2021-0194	Improper access control in the Intel(R) In-Band Manageability software before version 2.13.0 may allow a privileged user to potentially enable escalation of privilege via network access.	7.2	More Details
CVE-2022-30002	Insurance Management System 1.0 is vulnerable to SQL Injection via /insurance/editNominee.php?nominee_id=.	7.2	More Details
CVE-2022-30452	ShopWind <= v3.4.2 has a Sql injection vulnerability in Database.php	7.2	More Details
CVE-2022-1681	Authentication Bypass Using an Alternate Path or Channel in GitHub repository requarks/wiki prior to 2.5.281. User can get root user permissions	7.2	More Details
CVE-2021-27772	Users are able to read group conversations without actively taking part in them. Next to one to one conversations, users are able to start group conversations with multiple users. It was found possible to obtain the contents of these group conversations without being part of it. This could lead to information leakage where confidential information discussed in private groups is read by other users without the users knowledge.	7.1	More Details
CVE-2022-28184	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where an unprivileged regular user can access administrator- privileged registers, which may lead to denial of service, information disclosure, and data tampering.	7.1	More Details
CVE-2021-26362	A malicious or compromised UApp or ABL may be used by an attacker to issue a malformed system call which results in mapping sensitive System Management Network (SMN) registers leading to a loss of integrity and availability.	7.1	More Details
CVE-2021-26366	An attacker, who gained elevated privileges via some other vulnerability, may be able to read data from Boot ROM resulting in a loss of system integrity.	7.1	More Details
CVE-2022-1356	cnMaestro is vulnerable to a local privilege escalation. By default, a user does not have root privileges. However, a user can run scripts as sudo, which could allow an attacker to gain root privileges when running user scripts outside allowed commands.	7.1	More Details
CVE-2022-29368	Moddable commit before 135aa9a4a6a9b49b60aa730ebc3bcc6247d75c45 was discovered to contain an out-of-bounds read via the function fxUint8Getter at /moddable/xs/sources/xsDataView.c.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1714	Out-of-bounds Read in GitHub repository radareorg/radare2 prior to 5.7.0. The bug causes the program reads data past the end of the intented buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.	7.1	More Details
CVE-2022-22796	Sysaid – Sysaid System Takeover - An attacker can bypass the authentication process by accessing to: /wmiwizard.jsp, Then to: /ConcurrentLogin.jsp, then click on the login button, and it will redirect you to /home.jsp without any authentication.	7.0	More Details
CVE-2021-33077	Insufficient control flow management in firmware for some Intel(R) SSD, Intel(R) Optane(TM) SSD and Intel(R) SSD DC Products may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2021-33080	Exposure of sensitive system information due to uncleared debug information in firmware for some Intel(R) SSD DC, Intel(R) Optane(TM) SSD and Intel(R) Optane(TM) SSD DC Products may allow an unauthenticated user to potentially enable information disclosure or escalation of privilege via physical access.	6.8	More Details
CVE-2022-28185	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the ECC layer, where an unprivileged regular user can cause an out-of-bounds write, which may lead to denial of service and data tampering.	6.8	More Details
CVE-2022-29855	Mitel 6800 and 6900 Series SIP phone devices through 2022-04-27 have "undocumented functionality." A vulnerability in Mitel 6800 Series and 6900 Series SIP phones excluding 6970, versions 5.1 SP8 (5.1.0.8016) and earlier, and 6.0 (6.0.0.368) through 6.1 HF4 (6.1.0.165), could allow a unauthenticated attacker with physical access to the phone to gain root access due to insufficient access control for test functionality during system startup. A successful exploit could allow access to sensitive information and code execution.	6.8	More Details
CVE-2022-22798	Sysaid – Pro Plus Edition, SysAid Help Desk Broken Access Control v20.4.74 b10, v22.1.20 b62, v22.1.30 b49 - An attacker needs to log in as a guest after that the system redirects him to the service portal or EndUserPortal.JSP, then he needs to change the path in the URL to /ConcurrentLogin%2ejsp after that he will receive an error message with a login button, by clicking on it, he will connect to the system dashboard. The attacker can receive sensitive data like server details, usernames, workstations, etc. He can also perform actions such as uploading files, deleting calls from the system.	6.8	More Details
CVE-2021-44167	An incorrect permission assignment for critical resource vulnerability [CWE-732] in FortiClient for Linux version 6.0.8 and below, 6.2.9 and below, 6.4.7 and below, 7.0.2 and below may allow an unauthenticated attacker to access sensitive information in log files and directories via symbolic links.	6.8	More Details
CVE-2022-0004	Hardware debug modes and processor INIT setting that allow override of locks for some Intel(R) Processors in Intel(R) Boot Guard and Intel(R) TXT may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2022-29854	A vulnerability in Mitel 6900 Series IP (MiNet) phones excluding 6970, versions 1.8 (1.8.0.12) and earlier, could allow a unauthenticated attacker with physical access to the phone to gain root access due to insufficient access control for test functionality during system startup. A successful exploit could allow access to sensitive information and code execution.	6.8	More Details
CVE-2021-27770	The vulnerability was discovered within the “FaviconService”. The service takes a base64-encoded URL which is then requested by the webserver. We assume this service is used by the “meetings”-function where users can specify an external URL where the online meeting will take place.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0026	A local privilege escalation (PE) vulnerability exists in Palo Alto Networks Cortex XDR agent software on Windows that enables an authenticated local user with file creation privilege in the Windows root directory (such as C:\) to execute a program with elevated privileges. This issue impacts all versions of Cortex XDR agent without content update 330 or a later content update version.	6.7	More Details
CVE-2021-30361	The Check Point Gaia Portal's GUI Clients allowed authenticated administrators with permission for the GUI Clients settings to inject a command that would run on the Gaia OS.	6.7	More Details
CVE-2022-0025	A local privilege escalation (PE) vulnerability exists in Palo Alto Networks Cortex XDR agent software on Windows that enables an authenticated local user with file creation privilege in the Windows root directory (such as C:\) to execute a program with elevated privileges. This issue impacts: All versions of the Cortex XDR agent when upgrading to Cortex XDR agent 7.7.0 on Windows; Cortex XDR agent 7.7.0 without content update 500 or a later version on Windows. This issue does not impact other platforms or other versions of the Cortex XDR agent.	6.7	More Details
CVE-2021-33124	Out-of-bounds write in the BIOS authenticated code module for some Intel(R) Processors may allow a privileged user to potentially enable aescalation of privilege via local access.	6.7	More Details
CVE-2022-24382	Improper input validation in firmware for some Intel(R) NUCs may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-24297	Improper buffer restrictions in firmware for some Intel(R) NUCs may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-24910	A buffer overflow vulnerability exists in the httpd parse_ping_result API functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted file can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.	6.7	More Details
CVE-2021-33103	Unintended intermediary in the BIOS authenticated code module for some Intel(R) Processors may allow a privileged user to potentially enable aescalation of privilege via local access.	6.7	More Details
CVE-2022-21237	Improper buffer access in firmware for some Intel(R) NUCs may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-33108	Improper input validation in the Intel(R) In-Band Manageability software before version 2.13.0 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-28247	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an uncontrolled search path vulnerability that could lead to local privilege escalation. Exploitation of this issue requires user interaction in that a victim must run the uninstaller with Admin privileges.	6.7	More Details
CVE-2022-22975	An issue was discovered in the Pinniped Supervisor with either LADPIdentityProvider or ActiveDirectoryIdentityProvider resources. An attack would involve the malicious user changing the common name (CN) of their user entry on the LDAP or AD server to include special characters, which could be used to perform LDAP query injection on the Supervisor's LDAP query which determines their Kubernetes group membership.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30959	A missing permission check in Jenkins SSH Plugin 2.6.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified SSH server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2022-30381	Merchandise Online Store v1.0 is vulnerable to file deletion via /vloggers_merch/classes/Master.php?f=delete_img.	6.5	More Details
CVE-2022-30952	Jenkins Pipeline SCM API for Blue Ocean Plugin 1.25.3 and earlier allows attackers with Job/Configure permission to access credentials with attacker-specified IDs stored in the private per-user credentials stores of any attacker-specified user in Jenkins.	6.5	More Details
CVE-2022-30953	A cross-site request forgery (CSRF) vulnerability in Jenkins Blue Ocean Plugin 1.25.3 and earlier allows attackers to connect to an attacker-specified HTTP server.	6.5	More Details
CVE-2022-30954	Jenkins Blue Ocean Plugin 1.25.3 and earlier does not perform a permission check in several HTTP endpoints, allowing attackers with Overall/Read permission to connect to an attacker-specified HTTP server.	6.5	More Details
CVE-2022-30955	Jenkins GitLab Plugin 1.5.31 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	6.5	More Details
CVE-2022-30045	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_decode() performs incorrect memory handling while parsing crafted XML files, leading to a heap out-of-bounds read.	6.5	More Details
CVE-2022-1406	Improper input validation in GitLab CE/EE affecting all versions from 8.12 prior to 14.8.6, all versions from 14.9.0 prior to 14.9.4, and 14.10.0 allows a Developer to read protected Group or Project CI/CD variables by importing a malicious project	6.5	More Details
CVE-2022-1044	Sensitive Data Exposure Due To Insecure Storage Of Profile Image in GitHub repository polonel/trudesk prior to v1.2.1.	6.5	More Details
CVE-2022-22475	IBM WebSphere Application Server Liberty and Open Liberty 17.0.0.3 through 22.0.0.5 are vulnerable to identity spoofing by an authenticated user. IBM X-Force ID: 225603.	6.5	More Details
CVE-2022-30375	Sourcecodester Simple Social Networking Site v1.0 is vulnerable to file deletion via /sns/classes/Master.php?f=delete_img.	6.5	More Details
CVE-2022-30367	Air Cargo Management System v1.0 is vulnerable to file deletion via /acms/classes/Master.php?f=delete_img.	6.5	More Details
CVE-2022-22482	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.5 and 6.1.0.0 through 6.1.1.0 could allow an authenticated user to upload files that could fill up the filesystem and cause a denial of service. IBM X-Force ID: 225977.	6.5	More Details
CVE-2022-24584	Incorrect access control in Yubico OTP functionality of the YubiKey hardware tokens along with the Yubico OTP validation server. The Yubico OTP supposedly creates hardware bound second factor credentials. When a user reprograms the OTP functionality by "writing" it on a token using the Yubico Personalization Tool, they can then upload the new configuration to Yubicos OTP validation servers. NOTE: the vendor disputes this because there is no way for a YubiKey device to prevent a user from deciding that a secret value, which is imported into the device, should also be stored elsewhere	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1706	A vulnerability was found in Ignition where ignition configs are accessible from unprivileged containers in VMs running on VMware products. This issue is only relevant in user environments where the Ignition config contains secrets. The highest threat from this vulnerability is to data confidentiality. Possible workaround is to not put secrets in the Ignition config.	6.5	More Details
CVE-2022-24611	Denial of Service (DoS) in the Z-Wave S0 NonceGet protocol specification in Silicon Labs Z-Wave 500 series allows local attackers to block S0/S2 protected Z-Wave network via crafted S0 NonceGet Z-Wave packages, utilizing included but absent NodeIDs.	6.5	More Details
CVE-2022-1510	An issue has been discovered in GitLab affecting all versions starting from 13.9 before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. GitLab was not correctly handling malicious text in the CI Editor and CI Pipeline details page allowing the attacker to cause uncontrolled resource consumption.	6.5	More Details
CVE-2022-1560	The Amministrazione Aperta WordPress plugin before 3.8 does not validate the open parameter before using it in an include statement, leading to a Local File Inclusion issue. The original advisory mentions that unauthenticated users can exploit this, however the affected file generates a fatal error when accessed directly and the affected code is not reached. The issue can be exploited via the dashboard when logged in as an admin, or by making a logged in admin open a malicious link	6.5	More Details
CVE-2022-30408	Covid-19 Travel Pass Management System v1.0 is vulnerable to file deletion via /ctpms/classes/Master.php?f=delete_img.	6.5	More Details
CVE-2022-29332	D-LINK DIR-825 AC1200 R2 is vulnerable to Directory Traversal. An attacker could use the "../../../../" setting of the FTP server folder to set the router's root folder for FTP access. This allows you to access the entire router file system via the FTP server.	6.5	More Details
CVE-2022-1728	Allowing long password leads to denial of service in polonel/trudesk in GitHub repository polonel/trudesk prior to 1.2.2. This vulnerability can be abused by doing a DDoS attack for which genuine users will not able to access resources/applications.	6.5	More Details
CVE-2022-1398	The External Media without Import WordPress plugin through 1.1.2 does not have any authorisation and does to ensure that medias added via URLs are external medias, which could allow any authenticated users, such as subscriber to perform blind SSRF attacks	6.5	More Details
CVE-2022-23670	A remote authenticated information disclosure vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	6.5	More Details
CVE-2022-0578	Code Injection in GitHub repository publify/publify prior to 9.2.8.	6.5	More Details
CVE-2022-0574	Improper Access Control in GitHub repository publify/publify prior to 9.2.8.	6.5	More Details
CVE-2021-3611	A stack overflow vulnerability was found in the Intel HD Audio device (intel-hda) of QEMU. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition. The highest threat from this vulnerability is to system availability. This flaw affects QEMU versions prior to 7.0.0.	6.5	More Details
CVE-2021-42644	cmseasy V7.7.5_20211012 is affected by an arbitrary file read vulnerability. After login, the configuration file information of the website such as the database configuration file (config / config_database) can be read through this vulnerability.	6.5	More Details
CVE-2022-29977	There is an assertion failure error in stbi__jpeg_huff_decode, stb_image.h:1894 in libsixel img2sixel 1.8.6. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted JPEG file.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1407	The VikBooking Hotel Booking Engine & PMS WordPress plugin before 1.5.8 does not have CSRF check in place when adding a tracking campaign, and does not escape the campaign fields when outputting them In attributes. As a result, attackers could make a logged in admin add tracking campaign with XSS payloads in them via a CSRF attack	6.5	More Details
CVE-2022-24830	OpenClinica is an open source software for Electronic Data Capture (EDC) and Clinical Data Management (CDM). OpenClinica prior to version 3.16 is vulnerable to path traversal in multiple endpoints, leading to arbitrary file read/write, and potential remote code execution. There are no known workarounds. This issue has been patched and users are recommended to upgrade.	6.5	More Details
CVE-2022-29845	In Progress Ipswitch WhatsUp Gold 21.1.0 through 21.1.1, and 22.0.0, it is possible for an authenticated user to invoke an API transaction that would allow them to read the contents of a local file.	6.5	More Details
CVE-2022-29848	In Progress Ipswitch WhatsUp Gold 17.0.0 through 21.1.1, and 22.0.0, it is possible for an authenticated user to invoke an API transaction that would allow them to read sensitive operating-system attributes from a host that is accessible by the WhatsUp Gold system.	6.5	More Details
CVE-2022-22393	IBM WebSphere Application Server Liberty 17.0.0.3 through 22.0.0.5 , with the adminCenter-1.0 feature configured, could allow an authenticated user to issue a request to obtain the status of HTTP/HTTPS ports which are accessible by the application server. IBM X-Force ID: 222078.	6.5	More Details
CVE-2022-30059	Shopwind <=v3.4.2 was discovered to contain a Arbitrary File Delete vulnerability via the neirong parameter at \backend\controllers\DbController.php.	6.5	More Details
CVE-2022-30061	ftcms <=2.1 was discovered to be vulnerable to directory traversal attacks via the parameter tp.	6.5	More Details
CVE-2022-30062	ftcms <=2.1 was discovered to be vulnerable to Arbitrary File Read via tp.php	6.5	More Details
CVE-2022-29008	An insecure direct object reference (IDOR) vulnerability in the viewid parameter of Bus Pass Management System v1.0 allows attackers to access sensitive information.	6.5	More Details
CVE-2022-29978	There is a floating point exception error in sixel_encoder_do_resize, encoder.c:633 in libsixel img2sixel 1.8.6. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted JPEG file.	6.5	More Details
CVE-2021-36613	Mikrotik RouterOs before stable 6.48.2 suffers from a memory corruption vulnerability in the ptp process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	6.5	More Details
CVE-2021-46744	An attacker with access to a malicious hypervisor may be able to infer data values used in a SEV guest on AMD CPUs by monitoring ciphertext values over time.	6.5	More Details
CVE-2021-36614	Mikrotik RouterOs before stable 6.48.2 suffers from a memory corruption vulnerability in the tr069-client process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	6.5	More Details
CVE-2022-22971	In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26510	A firmware update vulnerability exists in the iburn firmware checks functionality of InHand Networks InRouter302 V3.5.37. A specially-crafted HTTP request can lead to firmware update. An attacker can send a sequence of requests to trigger this vulnerability.	6.5	More Details
CVE-2022-26020	An information disclosure vulnerability exists in the router configuration export functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted network request can lead to increased privileges. An attacker can send an HTTP request to trigger this vulnerability.	6.5	More Details
CVE-2022-28244	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) is affected by a violation of secure design principles through bypassing the content security policy, which could result in an attacker sending arbitrarily configured requests to the cross-origin attack target domain. Exploitation requires user interaction in which the victim needs to access a crafted PDF file on an attacker's server.	6.3	More Details
CVE-2021-27768	Using the ability to perform a Man-in-the-Middle (MITM) attack, which indicates a lack of hostname verification, sensitive account information was able to be intercepted. In this specific scenario, the application's network traffic was intercepted using a proxy server set up in 'transparent' mode while a certificate with an invalid hostname was active. The Android application was found to have hostname verification issues during the server setup and login flows; however, the application did not process requests post-login.	6.3	More Details
CVE-2022-21238	A cross-site scripting (xss) vulnerability exists in the info.jsp functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can send an HTTP request to trigger this vulnerability.	6.1	More Details
CVE-2022-23137	ZTE's ZXCDN product has a reflective XSS vulnerability. The attacker could modify the parameters in the content clearing request url, and when a user clicks the url, an XSS attack will be triggered.	6.1	More Details
CVE-2020-22987	Cross-Site Scripting (XSS) vulnerability in MicroStrategy Web SDK 10.11 and earlier, allows remote unauthenticated attackers to execute arbitrary code via the fileToUpload parameter to the uploadFile task.	6.1	More Details
CVE-2021-42648	Cross-site scripting (XSS) vulnerability exists in Coder Code-Server before 3.12.0, allows attackers to execute arbitrary code via crafted URL.	6.1	More Details
CVE-2022-1418	The Social Stickers WordPress plugin through 2.2.9 does not have CSRF checks in place when updating its Social Network settings, and does not escape some of these fields, which could allow attackers to make a logged-in admin change them and lead to Stored Cross-Site Scripting issues.	6.1	More Details
CVE-2021-43081	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiOS version 7.0.3 and below, 6.4.8 and below, 6.2.10 and below, 6.0.14 to 6.0.0. and in FortiProxy version 7.0.1 and below, 2.0.7 to 2.0.0 web filter override form may allow an unauthenticated attacker to perform an XSS attack via crafted HTTP GET requests.	6.1	More Details
CVE-2022-30770	Terminalfour versions 8.3.7, 8.3.x versions prior to version 8.3.8 and r 8.2.x versions prior to version 8.2.18.5 or 8.2.18.2.1 are vulnerable to (XSS) vulnerability that could be exploited by an attacker to mislead an administrator and steal their credentials.	6.1	More Details
CVE-2022-1436	The WPCargo Track & Trace WordPress plugin before 6.9.5 does not sanitise and escape the wpcargo_tracking_number parameter before outputting it back in the page, which could allow attackers to perform reflected Cross-Site Scripting attacks.	6.1	More Details
CVE-2022-28919	HTMLCreator release_stable_2020-07-29 was discovered to contain a cross-site scripting (XSS) vulnerability via the function _generateFilename.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1682	Reflected Xss using url based payload in GitHub repository neorazorx/facturascripts prior to 2022.07. Xss can use to steal user's cookies which lead to Account takeover or do any malicious activity in victim's browser	6.1	More Details
CVE-2020-22985	Cross-Site Scripting (XSS) vulnerability in MicroStrategy Web SDK 10.11 and earlier, allows remote unauthenticated attackers to execute arbitrary code via the key parameter to the getESRIExtraConfig task.	6.1	More Details
CVE-2020-22986	Cross-Site Scripting (XSS) vulnerability in MicroStrategy Web SDK 10.11 and earlier, allows remote unauthenticated attackers to execute arbitrary code via the searchString parameter to the wikiScrapper task.	6.1	More Details
CVE-2022-1465	The WPC Smart Wishlist for WooCommerce WordPress plugin before 2.9.9 does not sanitise and escape a parameter before outputting it back in an attribute via an AJAX action, leading to a Reflected Cross-Site Scripting issue.	6.1	More Details
CVE-2020-22984	Cross-Site Scripting (XSS) vulnerability in MicroStrategy Web SDK 10.11 and earlier, allows remote unauthenticated attackers to execute arbitrary code via key parameter to the getGoogleExtraConfig task.	6.1	More Details
CVE-2022-1267	The BMI BMR Calculator WordPress plugin through 1.3 does not sanitise and escape arbitrary POST data before outputting it back in the response, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-28818	ColdFusion versions CF2021U3 (and earlier) and CF2018U13 are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	6.1	More Details
CVE-2022-1217	The Custom TinyMCE Shortcode Button WordPress plugin through 1.1 does not sanitise and escape the PHP_SELF variable before outputting it back in an attribute in an admin page, leading to Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-1216	The Advanced Image Sitemap WordPress plugin through 1.2 does not sanitise and escape the PHP_SELF PHP variable before outputting it back in an attribute in an admin page, leading to Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-30777	Parallels H-Sphere 3.6.1713 allows XSS via the index_en.php from parameter.	6.1	More Details
CVE-2022-30776	atmail 6.5.0 allows XSS via the index.php/admin/index/ error parameter.	6.1	More Details
CVE-2022-1702	SonicWall SMA1000 series firmware 12.4.0, 12.4.1-02965 and earlier versions accept a user-controlled input that specifies a link to an external site and uses that link in a redirect which leads to Open redirection vulnerability.	6.1	More Details
CVE-2021-22531	A bug exist in the input parameter of Access Manager that allows supply of invalid character to trigger cross-site scripting vulnerability. This affects NetIQ Access Manager 4.5 and 5.0	6.1	More Details
CVE-2022-29728	Survey Sparrow Enterprise Survey Software 2022 has a Reflected cross-site scripting (XSS) vulnerability in the test parameter.	6.1	More Details
CVE-2022-28078	Home Owners Collection Management v1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in the Admin panel via the $_GET['page'] parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28077	Home Owners Collection Management v1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in the Admin panel via the $_GET['s'] parameter.	6.1	More Details
CVE-2022-1455	The Call Now Button WordPress plugin before 1.1.2 does not escape a parameter before outputting it back in an attribute of a hidden input, leading to a Reflected Cross-Site Scripting when the premium is enabled	6.1	More Details
CVE-2022-1460	An issue has been discovered in GitLab affecting all versions starting from 9.2 before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. GitLab was not performing correct authorizations on scheduled pipelines allowing a malicious user to run a pipeline in the context of another user.	6.1	More Details
CVE-2022-23706	A remote cross-site scripting (xss) vulnerability was discovered in HPE OneView version(s): Prior to 7.0. HPE has provided a software update to resolve this vulnerability in HPE OneView.	6.1	More Details
CVE-2022-30050	Gnuboard 5.55 and 5.56 is vulnerable to Cross Site Scripting (XSS) via bbs/member_confirm.php.	6.1	More Details
CVE-2022-28186	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where the product receives input or data, but does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly, which may lead to denial of service or data tampering.	6.1	More Details
CVE-2022-30489	WAVLINK WN535 G3 was discovered to contain a cross-site scripting (XSS) vulnerability via the hostname parameter at /cgi-bin/login.cgi.	6.1	More Details
CVE-2022-27656	The Web administration UI of SAP Web Dispatcher and the Internet Communication Manager (ICM) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2022-23166	Sysaid – Sysaid Local File Inclusion (LFI) – An unauthenticated attacker can access to the system by accessing to "/lib/tinymce/examples/index.html" path. in the "Insert/Edit Embedded Media" window Choose Type : iFrame and File/URL : [here is the LFI] Solution: Update to 22.2.20 cloud version, or to 22.1.64 on premise version.	6.1	More Details
CVE-2021-28290	A cross-site scripting (XSS) vulnerability in Skoruba IdentityServer4.Admin before 2.0.0 via unencoded value passed to the data-secret-value parameter.	6.1	More Details
CVE-2022-30110	The file preview functionality in Jirafeau < 4.4.0, which is enabled by default, could be exploited for cross site scripting. An attacker could upload image/svg+xml files containing JavaScript. When someone visits the File Preview URL for this file, the JavaScript inside of this image/svg+xml file will be executed in the users' browser.	6.1	More Details
CVE-2022-23659	A remote reflected cross site scripting (xss) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	6.1	More Details
CVE-2022-25172	An information disclosure vulnerability exists in the web interface session cookie functionality of InHand Networks InRouter302 V3.5.4. The session cookie misses the HttpOnly flag, making it accessible via JavaScript and thus allowing an attacker, able to perform an XSS attack, to steal the session cookie.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33021	xArrow SCADA versions 7.2 and prior is vulnerable to cross-site scripting due to parameter ‘edate’ of the resource xhisalarm.htm, which may allow an unauthorized attacker to execute arbitrary code.	6.1	More Details
CVE-2021-33001	xArrow SCADA versions 7.2 and prior is vulnerable to cross-site scripting due to parameter ‘bdate’ of the resource xhisvalue.htm, which may allow an unauthorized attacker to execute arbitrary code.	6.1	More Details
CVE-2022-1358	The affected On-Premise is vulnerable to data exfiltration through improper neutralization of special elements used in an SQL command. This could allow an attacker to exfiltrate and dump all data held in the cnMaestro database.	5.9	More Details
CVE-2022-29162	runc is a CLI tool for spawning and running containers on Linux according to the OCI specification. A bug was found in runc prior to version 1.1.2 where `runc exec --cap` created processes with non-empty inheritable Linux process capabilities, creating an atypical Linux environment and enabling programs with inheritable file capabilities to elevate those capabilities to the permitted set during execve(2). This bug did not affect the container security sandbox as the inheritable set never contained more capabilities than were included in the container's bounding set. This bug has been fixed in runc 1.1.2. This fix changes `runc exec --cap` behavior such that the additional capabilities granted to the process being executed (as specified via `--cap` arguments) do not include inheritable capabilities. In addition, `runc spec` is changed to not set any inheritable capabilities in the created example OCI spec (`config.json`) file.	5.9	More Details
CVE-2022-1359	The affected On-Premise cnMaestro is vulnerable to an arbitrary file-write through improper limitation of a pathname to a restricted directory inside a specific route. If an attacker supplied path traversal charters (../) as part of a filename, the server will save the file where the attacker chooses. This could allow an attacker to write any data to any file in the server.	5.7	More Details
CVE-2021-33025	xArrow SCADA versions 7.2 and prior permits unvalidated registry keys to be run with application-level privileges.	5.6	More Details
CVE-2022-28264	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-1623	LibTIFF master branch has an out-of-bounds read in LZWDecode in libtiff/tif_lzw.c:624, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit b4e79bfa.	5.5	More Details
CVE-2022-28254	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-28251	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28263	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-28262	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-26351	Insufficient DRAM address validation in System Management Unit (SMU) may result in a DMA (Direct Memory Access) read/write from/to invalid DRAM address that could result in denial of service.	5.5	More Details
CVE-2022-28265	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-28266	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-28253	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-28261	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-33117	Improper access control for some 3rd Generation Intel(R) Xeon(R) Scalable Processors before BIOS version MR7, may allow a local attacker to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-29017	Bento4 v1.6.0.0 was discovered to contain a segmentation fault via the component /x86_64/multiarch/strlen-avx2.S.	5.5	More Details
CVE-2022-28249	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28260	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-21147	An out of bounds read vulnerability exists in the malware scan functionality of ESTsoft Alyac 2.5.7.7. A specially-crafted PE file can trigger this vulnerability to cause denial of service and termination of malware scan. An attacker can provide a malicious file to trigger this vulnerability.	5.5	More Details
CVE-2021-33069	Improper resource shutdown or release in firmware for some Intel(R) SSD, Intel(R) SSD DC, Intel(R) Optane(TM) SSD and Intel(R) Optane(TM) SSD DC may allow a privileged user to potentially enable denial of service via local access.	5.5	More Details
CVE-2022-28255	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-28774	Under certain conditions, the SAP Host Agent logfile shows information which would otherwise be restricted.	5.5	More Details
CVE-2022-21151	Processor optimization removal or modification of security-critical code for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-30126	In Apache Tika, a regular expression in our StandardsText class, used by the StandardsExtractingContentHandler could lead to a denial of service caused by backtracking on a specially crafted file. This only affects users who are running the StandardsExtractingContentHandler, which is a non-standard handler. This is fixed in 1.28.2 and 2.4.0	5.5	More Details
CVE-2022-25169	The BPG parser in versions of Apache Tika before 1.28.2 and 2.4.0 may allocate an unreasonable amount of memory on carefully crafted files.	5.5	More Details
CVE-2022-28256	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by a use-after-free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-28259	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-28250	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by a use-after-free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28257	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-28258	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-30775	xpdf 4.04 allocates excessive memory when presented with crafted input. This can be triggered by (for example) sending a crafted PDF document to the pdftoppm binary. It is most easily reproduced with the DCMAKE_CXX_COMPILER=afl-clang-fast++ option.	5.5	More Details
CVE-2022-28267	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-1622	LibTIFF master branch has an out-of-bounds read in LZWDecode in libtiff/tif_lzw.c:619, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit b4e79bfa.	5.5	More Details
CVE-2022-28188	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where the product receives input or data, but does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly, which may lead to denial of service.	5.5	More Details
CVE-2022-28248	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-21131	Improper access control for some Intel(R) Xeon(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-28246	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-1674	NULL Pointer Dereference in function vim_regexec_string at regexp.c:2733 in GitHub repository vim/vim prior to 8.2.4938. NULL Pointer Dereference in function vim_regexec_string at regexp.c:2733 allows attackers to cause a denial of service (application crash) via a crafted input.	5.5	More Details
CVE-2022-30067	GIMP 2.10.30 and 2.99.10 are vulnerable to Buffer Overflow. Through a crafted XCF file, the program will allocate for a huge amount of memory, resulting in insufficient memory or program crash.	5.5	More Details
CVE-2022-29302	SolarView Compact ver.6.00 was discovered to contain a local file disclosure via /html/Solar_Ftp.php.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28830	Adobe Framemaker versions 2029u8 (and earlier) and 2020u4 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-33149	Observable behavioral discrepancy in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-28187	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where the memory management software does not release a resource after its effective lifetime has ended, which may lead to denial of service.	5.5	More Details
CVE-2022-28245	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-28189	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a NULL pointer dereference may lead to a system crash.	5.5	More Details
CVE-2021-26376	Insufficient checks in System Management Unit (SMU) FeatureConfig may result in reenabling features potentially resulting in denial of resources and/or denial of service.	5.5	More Details
CVE-2022-28190	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where improper input validation can cause denial of service.	5.5	More Details
CVE-2022-28191	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (nvidia.ko), where uncontrolled resource consumption can be triggered by an unprivileged regular user, which may lead to denial of service.	5.5	More Details
CVE-2021-26373	Insufficient bound checks in the System Management Unit (SMU) may result in a system voltage malfunction that could result in denial of resources and/or possibly denial of service.	5.5	More Details
CVE-2021-26348	Failure to flush the Translation Lookaside Buffer (TLB) of the I/O memory management unit (IOMMU) may lead an IO device to write to memory it should not be able to access, resulting in a potential loss of integrity.	5.5	More Details
CVE-2021-0155	Unchecked return value in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-23165	Sysaid – Sysaid 14.2.0 Reflected Cross-Site Scripting (XSS) - The parameter "helpPageName" used by the page "/help/treecontent.jsp" suffers from a Reflected Cross-Site Scripting vulnerability. For an attacker to exploit this Cross-Site Scripting vulnerability, it's necessary for the affected product to expose the Offline Help Pages. An attacker may gain access to sensitive information or execute client-side code in the browser session of the victim user. Furthermore, an attacker would require the victim to open a malicious link. An attacker may exploit this vulnerability in order to perform phishing attacks. The attacker can receive sensitive data like server details, usernames, workstations, etc. He can also perform actions such as uploading files, deleting calls from the system	5.5	More Details
CVE-2021-26372	Insufficient bound checks related to PCIE in the System Management Unit (SMU) may result in access to an invalid address space that could result in denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33135	Uncontrolled resource consumption in the Linux kernel drivers for Intel(R) SGX may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-26349	Failure to assign a new report ID to an imported guest may potentially result in an SEV-SNP guest VM being tricked into trusting a dishonest Migration Agent (MA).	5.5	More Details
CVE-2021-26364	Insufficient bounds checking in an SMU mailbox register could allow an attacker to potentially read outside of the SRAM address range which could result in an exception handling leading to a potential denial of service.	5.5	More Details
CVE-2022-22484	IBM Spectrum Protect Operations Center 8.1.12 and 8.1.13 could allow a local attacker to obtain sensitive information, caused by plain text user account passwords potentially being stored in the browser's application command history. By accessing browser history, an attacker could exploit this vulnerability to obtain other user accounts' passwords. IBM X-Force ID: 226322.	5.5	More Details
CVE-2021-26375	Insufficient General Purpose IO (GPIO) bounds check in System Management Unit (SMU) may result in access/updates from/to invalid address space that could result in denial of service.	5.5	More Details
CVE-2021-26339	A bug in AMD CPU’s core logic may allow for an attacker, using specific code from an unprivileged VM, to trigger a CPU core hang resulting in a potential denial of service. AMD believes the specific code includes a specific x86 instruction sequence that would not be generated by compilers.	5.5	More Details
CVE-2021-26361	A malicious or compromised User Application (UApp) or AGESA Boot Loader (ABL) could be used by an attacker to exfiltrate arbitrary memory from the ASP stage 2 bootloader potentially leading to information disclosure.	5.5	More Details
CVE-2022-21136	Improper input validation for some Intel(R) Xeon(R) Processors may allow a privileged user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-26378	Insufficient bound checks in the System Management Unit (SMU) may result in access to an invalid address space that could result in denial of service.	5.5	More Details
CVE-2021-26388	Improper validation of the BIOS directory may allow for searches to read beyond the directory table copy in RAM, exposing out of bounds memory contents, resulting in a potential denial of service.	5.5	More Details
CVE-2022-22325	IBM MQ (IBM MQ for HPE NonStop 8.1.0) can inadvertently disclose sensitive information under certain circumstances to a local user from a stack trace. IBM X-Force ID: 218853.	5.5	More Details
CVE-2022-28837	Acrobat Pro DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by a use-after-free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-1753	A vulnerability, which was classified as critical, was found in WoWonder. Affected is the file /requests.php which is responsible to handle group messages. The manipulation of the argument group_id allows posting messages in other groups. It is possible to launch the attack remotely but it might require authentication. A video explaining the attack has been disclosed to the public.	5.4	More Details
CVE-2022-30966	Jenkins Random String Parameter Plugin 1.0 and earlier does not escape the name and description of Random String parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29975	An Authenticated Reflected Cross-site scripting at CC Parameter was discovered in MDaemon before 22.0.0 .	5.4	More Details
CVE-2022-30967	Jenkins Selection tasks Plugin 1.0 and earlier does not escape the name and description of Script Selection task variable parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-23674	A remote authenticated stored cross-site scripting (xss) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	5.4	More Details
CVE-2022-29435	Cross-Site Request Forgery (CSRF) vulnerability in Alexander Stokmann's Code Snippets Extended plugin <= 1.4.7 on WordPress allows an attacker to delete or to turn on/off snippets.	5.4	More Details
CVE-2022-30968	Jenkins vboxwrapper Plugin 1.3 and earlier does not escape the name and description of VBox node parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-30965	Jenkins Promoted Builds (Simple) Plugin 1.9 and earlier does not escape the name and description of Promotion Level parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-29610	SAP NetWeaver Application Server ABAP allows an authenticated attacker to upload malicious files and delete (theme) data, which could result in Stored Cross-Site Scripting (XSS) attack.	5.4	More Details
CVE-2021-31330	A Cross-Site Scripting (XSS) vulnerability exists within Review Board versions 3.0.20 and 4.0 RC1 and earlier. An authenticated attacker may inject malicious Javascript code when using Markdown editing within the application which remains persistent.	5.4	More Details
CVE-2022-1726	Bootstrap Tables XSS vulnerability with Table Export plug-in when exportOptions: htmlContent is true in GitHub repository wenzhixin/bootstrap-table prior to 1.20.2. Disclosing session cookies, disclosing secure session data, exfiltrating data to third-parties.	5.4	More Details
CVE-2022-30956	Jenkins Rundeck Plugin 3.6.10 and earlier does not restrict URL schemes in Rundeck webhook submissions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to submit crafted Rundeck webhook payloads.	5.4	More Details
CVE-2022-30964	Jenkins Multiselect parameter Plugin 1.3 and earlier does not escape the name and description of Multiselect parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-30013	A stored cross-site scripting (XSS) vulnerability in the upload function of totaljs CMS 3.4.5 allows attackers to execute arbitrary web scripts via a JavaScript embedded PDF file.	5.4	More Details
CVE-2021-39059	IBM Jazz Foundation (IBM Jazz Team Server 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 214619.	5.4	More Details
CVE-2022-30970	Jenkins Autocomplete Parameter Plugin 1.1 and earlier references Dropdown Autocomplete parameter and Auto Complete String parameter names in an unsafe manner from Javascript embedded in view definitions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1557	The ULeak Security & Monitoring WordPress plugin through 1.2.3 does not have authorisation and CSRF checks when updating its settings, and is also lacking sanitisation as well as escaping in some of them, which could allow any authenticated users such as subscriber to perform Stored Cross-Site Scripting attacks against admins viewing the settings	5.4	More Details
CVE-2022-30962	Jenkins Global Variable String Parameter Plugin 1.2 and earlier does not escape the name and description of Global Variable String parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-29727	Survey Sparrow Enterprise Survey Software 2022 has a Stored cross-site scripting (XSS) vulnerability in the Signup parameter.	5.4	More Details
CVE-2022-30960	Jenkins Application Detector Plugin 1.0.8 and earlier does not escape the name of Chois Application Version parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-1051	The WPQA Builder Plugin WordPress plugin before 5.2, used as a companion plugin for the Discy and Himer , does not sanitise and escape the city, phone or profile credentials fields when outputting it in the profile page, allowing any authenticated user to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-30073	WBCE CMS 1.5.2 is vulnerable to Cross Site Scripting (XSS) via /admin/users/save.php.	5.4	More Details
CVE-2022-30961	Jenkins Autocomplete Parameter Plugin 1.1 and earlier does not escape the name of Dropdown Autocomplete and Auto Complete String parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-1393	The WP Subtitle WordPress plugin before 3.4.1 adds a subtitle field and provides a shortcode to display it via [wp_subtitle]. The subtitle is stored as a custom post meta with the key: "wps_subtitle", which is sanitized upon post save/update, however is not sanitized when updating it directly from the post meta update button (via AJAX) - and this makes the XSS exploitable by authenticated users with a role as low as contributor.	5.4	More Details
CVE-2021-42943	Stored cross-site scripting (XSS) in admin/usermanager.php over IPPlan v4.92b allows remote attackers to inject arbitrary web script or HTML via the userid parameter.	5.4	More Details
CVE-2022-30057	Shopwind <=v3.4.2 was discovered to contain a stored cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2022-29976	An Authenticated Reflected Cross-site scripting at BCC Parameter was discovered in MDaemon before 22.0.0 .	5.4	More Details
CVE-2022-30072	WBCE CMS 1.5.2 is vulnerable to Cross Site Scripting (XSS) via \admin\pages\sections_save.php namesection2 parameters.	5.4	More Details
CVE-2022-30963	Jenkins JDK Parameter Plugin 1.0 and earlier does not escape the name and description of JDK parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29846	In Progress Ipswitch WhatsUp Gold 16.1 through 21.1.1, and 22.0.0, it is possible for an unauthenticated attacker to obtain the WhatsUp Gold installation serial number.	5.3	More Details
CVE-2022-27247	onlinetolls in cdSoft Onlinetools-Smart Winhotel.MX 2021 allows an attacker to download sensitive information about any customer (e.g., data of birth, full address, mail information, and phone number) via GastKont Insecure Direct Object Reference.	5.3	More Details
CVE-2022-30058	Shopwind <=v3.4.2 was discovered to contain a Arbitrary File Download vulnerability via the neirong parameter at \backend\controllers\DbController.php.	5.3	More Details
CVE-2022-30949	Jenkins REPO Plugin 1.14.0 and earlier allows attackers able to configure pipelines to check out some SCM repositories stored on the Jenkins controller's file system using local paths as SCM URLs, obtaining limited information about other projects' SCM contents.	5.3	More Details
CVE-2022-30689	HashiCorp Vault and Vault Enterprise from 1.10.0 to 1.10.2 did not correctly configure and enforce MFA on login after server restarts. This affects the Login MFA feature introduced in Vault and Vault Enterprise 1.10.0 and does not affect the separate Enterprise MFA feature set. Fixed in 1.10.3.	5.3	More Details
CVE-2022-29538	RESI Gemini-Net Web 4.2 is affected by Improper Access Control in authorization logic. An unauthenticated user is able to access some critical resources.	5.3	More Details
CVE-2021-27769	Information leakage occurs when a website reveals information that could aid an attacker to further exploit the system. This information may or may not be sensitive and does not automatically mean a breach is likely to occur. Overall, any information that could be used for an attack should be limited whenever possible.	5.3	More Details
CVE-2021-29726	IBM Sterling Secure Proxy 6.0.3 and IBM Secure External Authentication Server 6.0.3 does not properly ensure that a certificate is actually associated with the host due to improper validation of certificates. IBM X-Force ID: 201104.	5.3	More Details
CVE-2022-1352	Due to an insecure direct object reference vulnerability in Gitlab EE/CE affecting all versions from 11.0 prior to 14.8.6, 14.9 prior to 14.9.4, and 14.10 prior to 14.10.1, an endpoint may reveal the issue title to a user who crafted an API call with the ID of the issue from a public project that restricts access to issue only to project members.	5.3	More Details
CVE-2020-4957	IBM Security Identity Governance and Intelligence 5.2.6 could disclose sensitive information in URL parameters that could aid in future attacks against the system. IBM X-Force ID: 192208.	5.3	More Details
CVE-2022-22970	In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.	5.3	More Details
CVE-2021-46785	The Property module has a vulnerability in permission control.This vulnerability can be exploited to obtain the unique device identifier.	5.3	More Details
CVE-2022-1362	The affected On-Premise cnMaestro is vulnerable inside a specific route where a user can upload a crafted package to the system. An attacker could abuse this user-controlled data to execute arbitrary commands on the server.	5.0	More Details
CVE-2022-23668	A remote authenticated server-side request forgery (ssrf) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manage that address this security vulnerability.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1553	Leaking password protected articles content due to improper access control in GitHub repository publify/publify prior to 9.2.8. Attackers can leverage this vulnerability to view the contents of any password-protected article present on the publify website, compromising confidentiality and integrity of users.	4.9	More Details
CVE-2022-23675	A remote authenticated stored cross-site scripting (xss) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): 6.10.4 and below, 6.9.9 and below, 6.8.9-HF2 and below, 6.7.x and below. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	4.8	More Details
CVE-2022-1265	The BulletProof Security WordPress plugin before 6.1 does not sanitize and escape some of its CAPTCHA settings, which could allow high-privileged users to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-1435	The WPCargo Track & Trace WordPress plugin before 6.9.5 does not sanitize and escapes some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	4.8	More Details
CVE-2022-1512	The ScrollReveal.js Effects WordPress plugin through 1.2 does not sanitise and escape its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-0873	The Gmedia Photo Gallery WordPress plugin before 1.20.0 does not sanitise and escape the Album's name before outputting it in pages/posts with a media embed, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered-html capability is disallowed	4.8	More Details
CVE-2022-22320	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 218367.	4.8	More Details
CVE-2022-1334	The WP YouTube Live WordPress plugin before 1.8.3 does not validate, sanitise and escape various of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2013-10001	A vulnerability was found in HTC One/Sense 4.x. It has been rated as problematic. Affected by this issue is the certification validation of the mail client. An exploit has been disclosed to the public and may be used.	4.8	More Details
CVE-2022-1408	The VikBooking Hotel Booking Engine & PMS WordPress plugin before 1.5.8 does not escape various settings before outputting them in attributes, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-1062	The th23 Social WordPress plugin through 1.2.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1089	The Bulk Edit and Create User Profiles WordPress plugin before 1.5.14 does not sanitise and escape the Users Login, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1559	The Clipr WordPress plugin through 1.2.3 does not sanitise and escape its API Key settings before outputting it in an attribute, leading to a Stored Cross-Site Scripting issue even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-28920	Tieba-Cloud-Sign v4.9 was discovered to contain a cross-site scripting (XSS) vulnerability via the function strip_tags.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33075	Race condition in firmware for some Intel(R) Optane(TM) SSD, Intel(R) Optane(TM) SSD DC and Intel(R) SSD DC Products may allow a privileged user to potentially enable denial of service via local access.	4.7	More Details
CVE-2021-26347	Failure to validate the integer operand in ASP (AMD Secure Processor) bootloader may allow an attacker to introduce an integer overflow in the L2 directory table in SPI flash resulting in a potential denial of service.	4.7	More Details
CVE-2022-29436	Persistent Cross-Site Scripting (XSS) vulnerability in Alexander Stokmann's Code Snippets Extended plugin <= 1.4.7 on WordPress via Cross-Site Request Forgery (vulnerable parameters &title, &snippet_code).	4.7	More Details
CVE-2021-33078	Race condition within a thread in firmware for some Intel(R) Optane(TM) SSD and Intel(R) SSD DC Products may allow a privileged user to potentially enable denial of service via local access.	4.7	More Details
CVE-2021-26350	A TOCTOU race condition in SMU may allow for the caller to obtain and manipulate the address of a message port register which may result in a potential denial of service.	4.7	More Details
CVE-2021-33082	Sensitive information in resource not removed before reuse in firmware for some Intel(R) SSD and Intel(R) Optane(TM) SSD Products may allow an unauthenticated user to potentially enable information disclosure via physical access.	4.6	More Details
CVE-2022-29927	In JetBrains TeamCity before 2022.04 reflected XSS on the Build Chain Status page was possible	4.6	More Details
CVE-2021-33074	Protection mechanism failure in firmware for some Intel(R) SSD, Intel(R) SSD DC and Intel(R) Optane(TM) SSD Products may allow an unauthenticated user to potentially enable information disclosure via physical access.	4.6	More Details
CVE-2021-33130	Insecure default variable initialization of Intel(R) RealSense(TM) ID Solution F450 before version 2.6.0.74 may allow an unauthenticated user to potentially enable information disclosure via physical access.	4.6	More Details
CVE-2022-22797	Sysaid – sysaid Open Redirect - An Attacker can change the redirect link at the parameter "redirectURL" from"GET" request from the url location: /CommunitySSORedirect.jsp?redirectURL=https://google.com. Unvalidated redirects and forwards are possible when a web application accepts untrusted input that could cause the web application to redirect the request to a URL contained within untrusted input. By modifying untrusted URL input to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.	4.6	More Details
CVE-2021-26363	A malicious or compromised UApp or ABL could potentially change the value that the ASP uses for its reserved DRAM, to one outside of the fenced area, potentially leading to data exposure.	4.4	More Details
CVE-2022-29928	In JetBrains TeamCity before 2022.04 leak of secrets in TeamCity agent logs was possible	4.4	More Details
CVE-2021-26368	Insufficient check of the process type in Trusted OS (TOS) may allow an attacker with privileges to enable a lesser privileged process to unmap memory owned by a higher privileged process resulting in a denial of service.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0486	Improper file permissions in the CommandPost, Collector, Sensor, and Sandbox components of Fidelis Network and Deception enables an attacker with local, administrative access to the CLI to modify affected files and enable escalation of privileges equivalent to the root user. The vulnerability is present in Fidelis Network and Deception versions prior to 9.4.5. Patches and updates are available to address this vulnerability.	4.4	More Details
CVE-2021-33083	Improper authentication in firmware for some Intel(R) SSD, Intel(R) Optane(TM) SSD, Intel(R) Optane(TM) SSD DC and Intel(R) SSD DC Products may allow an privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2022-1425	The WPQA Builder Plugin WordPress plugin before 5.2, used as a companion plugin for the Discy and Himer , does not validate that the message_id of the wpqa_message_view ajax action belongs to the requesting user, leading to any user being able to read messages for any other users via a Insecure Direct Object Reference (IDOR) vulnerability.	4.3	More Details
CVE-2021-23266	An anonymous user can craft a URL with text that ends up in the log viewer as is. The text can then include textual messages to mislead the administrator.	4.3	More Details
CVE-2022-28873	A vulnerability affecting F-Secure SAFE browser was discovered. An attacker can potentially exploit Javascript window.open functionality in SAFE Browser which could lead address bar spoofing attacks.	4.3	More Details
CVE-2022-28872	A vulnerability affecting F-Secure SAFE browser was discovered. A maliciously crafted website could make a phishing attack with address bar spoofing as the address bar was not correct if navigation fails in a loop.	4.3	More Details
CVE-2022-1545	It was possible to disclose details of confidential notes created via the API in Gitlab CE/EE affecting all versions from 13.2 prior to 14.8.6, 14.9 prior to 14.9.4, and 14.10 prior to 14.10.1 if an unauthorised project member was tagged in the note.	4.3	More Details
CVE-2022-1124	An improper authorization issue has been discovered in GitLab CE/EE affecting all versions prior to 14.8.6, all versions from 14.9.0 prior to 14.9.4, and 14.10.0, allowing Guest project members to access trace log of jobs when it is enabled	4.3	More Details
CVE-2022-30946	A cross-site request forgery (CSRF) vulnerability in Jenkins Script Security Plugin 1158.v7c1b_73a_69a_08 and earlier allows attackers to have Jenkins send an HTTP request to an attacker-specified webserver.	4.3	More Details
CVE-2022-30957	A missing permission check in Jenkins SSH Plugin 2.6.1 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2022-0027	An improper authorization vulnerability in Palo Alto Network Cortex XSOAR software enables authenticated users in non-Read-Only groups to generate an email report that contains summary information about all incidents in the Cortex XSOAR instance, including incidents to which the user does not have access. This issue impacts: All versions of Cortex XSOAR 6.1; All versions of Cortex XSOAR 6.2; All versions of Cortex XSOAR 6.5; Cortex XSOAR 6.6 versions earlier than Cortex XSOAR 6.6.0 build 6.6.0.2585049.	4.3	More Details
CVE-2022-1428	An issue has been discovered in GitLab affecting all versions before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. GitLab was incorrectly verifying throttling limits for authenticated package requests which resulted in limits not being enforced.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1349	The WPQA Builder Plugin WordPress plugin before 5.2, used as a companion plugin for the Discy and Himer , does not validate that the value passed to the image_id parameter of the ajax action wpqa_remove_image belongs to the requesting user, allowing any users (with privileges as low as Subscriber) to delete the profile pictures of any other user.	4.3	More Details
CVE-2022-29613	Due to insufficient input validation, SAP Employee Self Service allows an authenticated attacker with user privileges to alter employee number. On successful exploitation, the attacker can view personal details of other users causing a limited impact on confidentiality of the application.	4.3	More Details
CVE-2021-35249	This broken access control vulnerability pertains specifically to a domain admin who can access configuration & user data of other domains which they should not have access to. Please note the admin is unable to modify the data (read only operation). This UAC issue leads to a data leak to unauthorized users for a domain, with no log of them accessing the data unless they attempt to modify it. This read-only activity is logged to the original domain and does not specify which domain was accessed.	4.3	More Details
CVE-2021-27773	This vulnerability allows users to execute a clickjacking attack in the meeting's chat.	4.2	More Details
CVE-2022-29433	Authenticated (contributor or higher role) Cross-Site Scripting (XSS) vulnerability in Donations plugin <= 1.8 on WordPress.	4.1	More Details
CVE-2022-28192	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (nvidia.ko), where it may lead to a use-after-free, which in turn may cause denial of service. This attack is complex to carry out because the attacker needs to have control over freeing some host side resources out of sequence, which requires elevated privileges.	4.1	More Details
CVE-2022-25862	This affects the package sds from 0.0.0. The library could be tricked into adding or modifying properties of the Object.prototype by abusing the set function located in js/set.js. **Note:** This vulnerability derives from an incomplete fix to [CVE-2020-7618](https://security.snyk.io/vuln/SNYK-JS-SDS-564123)	4.0	More Details
CVE-2022-29587	Konica Minolta bizhub MFP devices before 2022-04-14 have an internal Chromium browser that executes with root (aka superuser) access privileges.	4.0	More Details
CVE-2021-26400	AMD processors may speculatively re-order load instructions which can result in stale data being observed when multiple processors are operating on shared memory, resulting in potential data leakage.	4.0	More Details
CVE-2022-0997	Improper file permissions in the CommandPost, Collector, and Sensor components of Fidelis Network and Deception enables an attacker with local, administrative access to the CLI to modify affected script files, which could result in arbitrary commands being run as root upon subsequent logon by a root user. The vulnerability is present in Fidelis Network and Deception versions prior to 9.4.5. Patches and updates are available to address this vulnerability.	3.9	More Details
CVE-2022-29929	In JetBrains TeamCity before 2022.04 potential XSS via Referrer header was possible	3.7	More Details
CVE-2021-23265	A logged-in and authenticated user with a Reviewer Role may lock a content item.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28252	Acrobat Reader DC version 22.001.2011x (and earlier), 20.005.3033x (and earlier) and 17.012.3022x (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	3.3	More Details
CVE-2021-26342	In SEV guest VMs, the CPU may fail to flush the Translation Lookaside Buffer (TLB) following a particular sequence of operations that includes creation of a new virtual machine control block (VMCB). The failure to flush the TLB may cause the microcode to use stale TLB translations which may allow for disclosure of SEV guest memory contents. Users of SEV-ES/SEV-SNP guest VMs are not impacted by this vulnerability.	3.3	More Details
CVE-2022-1722	SSRF in editor's proxy via IPv6 link-local address in GitHub repository jgraph/drawio prior to 18.0.5. SSRF to internal link-local IPv6 addresses	3.3	More Details
CVE-2022-1433	An issue has been discovered in GitLab affecting all versions starting from 14.4 before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. Missing invalidation of Markdown caching causes potential payloads from a previously exploitable XSS vulnerability (CVE-2022-1175) to persist and execute.	2.6	More Details
CVE-2022-0005	Sensitive information accessible by physical probing of JTAG interface for some Intel(R) Processors with SGX may allow an unprivileged user to potentially enable information disclosure via physical access.	2.4	More Details
CVE-2022-24890	Nextcloud Talk is a video and audio conferencing app for Nextcloud. In versions prior to 13.0.5 and 14.0.0, a call moderator can indirectly enable user webcams by granting permissions, if they were enabled before removing the permissions. A patch is available in versions 13.0.5 and 14.0.0. There are currently no known workarounds.	2.4	More Details
CVE-2022-1426	An issue has been discovered in GitLab affecting all versions starting from 12.6 before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. GitLab was not correctly authenticating a user that had some certain amount of information which allowed an user to authenticate without a personal access token.	2.0	More Details
CVE-2022-28235	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of the acroform event that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28238	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of annotations that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27802	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of annotations that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28237	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of annotations that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28233	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of annotations that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28230	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of the acroform event that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-42966	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-2022-27801	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of annotations that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27788	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28824	Adobe Framemaker versions 2029u8 (and earlier) and 2020u4 (and earlier) are affected by a Use-after-free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28823	Adobe Framemaker versions 2029u8 (and earlier) and 2020u4 (and earlier) are affected by a Use-after-free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28822	Adobe Framemaker versions 2029u8 (and earlier) and 2020u4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28821	Adobe Framemaker versions 2029u8 (and earlier) and 2020u4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27790	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of fonts that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27789	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of the acroform event that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27787	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28827	Adobe Framemaker versions 2029u8 (and earlier) and 2020u4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27786	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of fonts that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27785	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of fonts that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-24104	Acrobat Reader DC versions 20.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28819	Adobe Character Animator versions 4.4.2 (and earlier) and 22.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious SVG file.	N/A	More Details
CVE-2022-24103	Acrobat Reader DC versions 20.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-24101	Acrobat Reader DC versions 20.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28825	Adobe Framemaker versions 2029u8 (and earlier) and 2020u4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28828	Adobe Framemaker versions 2029u8 (and earlier) and 2020u4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27800	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of annotations that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28268	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27799	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of the acroform event that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27798	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27797	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of annotations that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-41927	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-2022-30779	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-2022-30778	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-2022-28269	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of Annotation objects that could result in a memory leak in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28829	Adobe Framemaker versions 2029u8 (and earlier) and 2020u4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27796	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of the acroform event that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27795	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of the acroform event that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27793	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27792	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-27791	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) is affected by a stack-based buffer overflow vulnerability due to insecure processing of a font, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28232	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) are affected by a use-after-free vulnerability in the processing of the collab object that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-28231	Acrobat Reader DC versions 22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier) is affected by an out-of-bounds read vulnerability when processing a doc object, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details