SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 11 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-2022-30292	Heap-based buffer overflow in sqbaselib.cpp in SQUIRREL 3.2 due to lack of a certain sq_reservestack call.	10.0	More Details
CVE-2022-24884	ecdsautils is a tiny collection of programs used for ECDSA (keygen, sign, verify). `ecdsa_verify_[prepare_]legacy()` does not check whether the signature values `r` and `s` are non-zero. A signature consisting only of zeroes is always considered valid, making it trivial to forge signatures. Requiring multiple signatures from different public keys does not mitigate the issue: `ecdsa_verify_list_legacy()` will accept an arbitrary number of such forged signatures. Both the `ecdsautil verify` CLI command and the libecdsautil library are affected. The issue has been fixed in ecdsautils 0.4.1. All older versions of ecdsautils (including versions before the split into a library and a CLI utility) are vulnerable.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42645	CMSimple_XH 1.7.4 is affected by a remote code execution (RCE) vulnerability. To exploit this vulnerability, an attacker must use the "File" parameter to upload a PHP payload to get a reverse shell from the vulnerable host.	10.0	More Details
CVE-2022-24877	Flux is an open and extensible continuous delivery solution for Kubernetes. Path Traversal in the kustomize-controller via a malicious `kustomization.yaml` allows an attacker to expose sensitive data from the controller's pod filesystem and possibly privilege escalation in multi-tenancy deployments. Workarounds include automated tooling in the user's CI/CD pipeline to validate `kustomization.yaml` files conform with specific policies. This vulnerability is fixed in kustomize-controller v0.24.0 and included in flux2 v0.29.0.	9.9	More Details
CVE-2022-29176	Rubygems is a package registry used to supply software for the Ruby language ecosystem. Due to a bug in the yank action, it was possible for any RubyGems.org user to remove and replace certain gems even if that user was not authorized to do so. To be vulnerable, a gem needed: one or more dashes in its name creation within 30 days OR no updates for over 100 days At present, we believe this vulnerability has not been exploited. RubyGems.org sends an email to all gem owners when a gem version is published or yanked. We have not received any support emails from gem owners indicating that their gem has been yanked without authorization. An audit of gem changes for the last 18 months did not find any examples of this vulnerability being used in a malicious way. A deeper audit for any possible use of this exploit is ongoing, and we will update this advisory once it is complete. Using Bundler in --frozen or --deployment mode in CI and during deploys, as the Bundler team has always recommended, will guarantee that your application does not silently switch to versions created using this exploit. To audit your application history for possible past exploits, review your Gemfile.lock and look for gems whose platform changed when the version number did not change. For example, gemname-3.1.2 updating to gemname-3.1.2-java could indicate a possible abuse of this vulnerability. RubyGems.org has been patched and is no longer vulnerable to this issue as of the 5th of May 2022.	9.9	More Details
CVE-2022-20779	Multiple vulnerabilities in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an attacker to escape from the guest virtual machine (VM) to the host machine, inject commands that execute at the root level, or leak system data from the host to the VM. For more information about these vulnerabilities, see the Details section of this advisory.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20777	Multiple vulnerabilities in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an attacker to escape from the guest virtual machine (VM) to the host machine, inject commands that execute at the root level, or leak system data from the host to the VM. For more information about these vulnerabilities, see the Details section of this advisory.	9.9	More Details
CVE-2022-24817	Flux2 is an open and extensible continuous delivery solution for Kubernetes. Flux2 versions between 0.1.0 and 0.29.0, helm-controller 0.1.0 to v0.19.0, and kustomize-controller 0.1.0 to v0.23.0 are vulnerable to Code Injection via malicious Kubeconfig. In multi-tenancy deployments this can also lead to privilege escalation if the controller's service account has elevated permissions. Workarounds include disabling functionality via Validating Admission webhooks by restricting users from setting the `spec.kubeConfig` field in Flux `Kustomization` and `HelmRelease` objects. Additional mitigations include applying restrictive AppArmor and SELinux profiles on the controller’s pod to limit what binaries can be executed. This vulnerability is fixed in kustomize-controller v0.23.0 and helm-controller v0.19.0, both included in flux2 v0.29.0	9.9	More Details
CVE-2022-20780	Multiple vulnerabilities in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an attacker to escape from the guest virtual machine (VM) to the host machine, inject commands that execute at the root level, or leak system data from the host to the VM. For more information about these vulnerabilities, see the Details section of this advisory.	9.9	More Details
CVE-2022-28895	A command injection vulnerability in the component /setnetworksettings/IPAddress of D-Link DIR882 DIR882A1_FW130B06 allows attackers to escalate privileges to root via a crafted payload.	9.8	More Details
CVE-2022-28906	TOTOLink N600R V5.3c.7159_B20190425 was discovered to contain a command injection vulnerability via the langtype parameter in /setting/setLanguageCfg.	9.8	More Details
CVE-2022-28907	TOTOLink N600R V5.3c.7159_B20190425 was discovered to contain a command injection vulnerability via the hosttime function in /setting/NTPSyncWithHost.	9.8	More Details
CVE-2022-28908	TOTOLink N600R V5.3c.7159_B20190425 was discovered to contain a command injection vulnerability via the ipdoamin parameter in /setting/setDiagnosisCfg.	9.8	More Details
CVE-2022-28909	TOTOLink N600R V5.3c.7159_B20190425 was discovered to contain a command injection vulnerability via the webwlanidx parameter in /setting/setWebWlanIdx.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28910	TOTOLink N600R V5.3c.7159_B20190425 was discovered to contain a command injection vulnerability via the devicename parameter in /setting/setDeviceName.	9.8	More Details
CVE-2022-28901	A command injection vulnerability in the component /SetTriggerLEDBlink/Blink of D-Link DIR882 DIR882A1_FW130B06 allows attackers to escalate privileges to root via a crafted payload.	9.8	More Details
CVE-2022-28896	A command injection vulnerability in the component /setnetworksettings/SubnetMask of D-Link DIR882 DIR882A1_FW130B06 allows attackers to escalate privileges to root via a crafted payload.	9.8	More Details
CVE-2022-28911	TOTOLink N600R V5.3c.7159_B20190425 was discovered to contain a command injection vulnerability via the filename parameter in /setting/CloudACMunualUpdate.	9.8	More Details
CVE-2022-28905	TOTOLink N600R V5.3c.7159_B20190425 was discovered to contain a command injection vulnerability via the devicemac parameter in /setting/setDeviceName.	9.8	More Details
CVE-2021-43163	A Remote Code Execution (RCE) vulnerability exists in Ruijie Networks Ruijie RG-EW Series Routers up to ReyeeOS 1.55.1915 / EW_3.0(1)B11P55 via the checkNet function in /cgi-bin/luci/api/auth.	9.8	More Details
CVE-2022-29591	Tenda TX9 Pro 22.03.02.10 devices have a SetNetControlList buffer overflow.	9.8	More Details
CVE-2022-28913	TOTOLink N600R V5.3c.7159_B20190425 was discovered to contain a command injection vulnerability via the filename parameter in /setting/setUploadSetting.	9.8	More Details
CVE-2022-28110	Hotel Management System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter at the login page.	9.8	More Details
CVE-2021-43094	An SQL Injection vulnerability exists in OpenMRS Reference Application Standalone Edition <=2.11 and Platform Standalone Edition <=2.4.0 via GET requests on arbitrary parameters in patient.page.	9.8	More Details
CVE-2022-30335	Bonanza Wealth Management System (BWM) 7.3.2 allows SQL injection via the login form. Users who supply the application with a SQL injection payload in the User Name textbox could collect all passwords in encrypted format from the Microsoft SQL Server component.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28738	A double free was found in the Regexp compiler in Ruby 3.x before 3.0.4 and 3.1.x before 3.1.2. If a victim attempts to create a Regexp from untrusted user input, an attacker may be able to write to unexpected memory locations.	9.8	More Details
CVE-2022-27412	Explore CMS v1.0 was discovered to contain a SQL injection vulnerability via a /page.php?id= request.	9.8	More Details
CVE-2022-1013	The Personal Dictionary WordPress plugin before 1.3.4 fails to properly sanitize user supplied POST data before it is being interpolated in an SQL statement and then executed, leading to a blind SQL injection vulnerability.	9.8	More Details
CVE-2022-0948	The Order Listener for WooCommerce WordPress plugin before 3.2.2 does not sanitise and escape the id parameter before using it in a SQL statement via a REST route available to unauthenticated users, leading to an SQL injection	9.8	More Details
CVE-2022-28912	TOTOLink N600R V5.3c.7159_B20190425 was discovered to contain a command injection vulnerability via the filename parameter in /setting/setUpgradeFW.	9.8	More Details
CVE-2022-29322	D-Link DIR-816 A2_v1.10CNB04 was discovered to contain a stack overflow via the IPADDR and nvmacaddr parameters in /goform/form2Dhcpip.	9.8	More Details
CVE-2022-28915	D-Link DIR-816 A2_v1.10CNB04 was discovered to contain a command injection vulnerability via the admuser and admpass parameters in /goform/setSysAdm.	9.8	More Details
CVE-2022-29321	D-Link DIR-816 A2_v1.10CNB04 was discovered to contain a stack overflow via the lanip parameter in /goform/setNetworkLan.	9.8	More Details
CVE-2022-26937	Windows Network File System Remote Code Execution Vulnerability	9.8	More Details
CVE-2022-22012	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	9.8	More Details
CVE-2022-20120	Product: AndroidVersions: Android kernelAndroid ID: A-203213034References: N/A	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29399	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a stack overflow via the url parameter in the function FUN_00415bf0.	9.8	More Details
CVE-2022-29398	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a stack overflow via the File parameter in the function FUN_0041309c.	9.8	More Details
CVE-2022-29397	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a stack overflow via the comment parameter in the function FUN_004196c8.	9.8	More Details
CVE-2022-29396	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a stack overflow via the comment parameter in the function FUN_00418f10.	9.8	More Details
CVE-2022-29395	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a stack overflow via the apcliKey parameter in the function FUN_0041bac4.	9.8	More Details
CVE-2022-29394	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a stack overflow via the macAddress parameter in the function FUN_0041b448.	9.8	More Details
CVE-2022-29393	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a stack overflow via the comment parameter in the function FUN_004192cc.	9.8	More Details
CVE-2022-29392	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a stack overflow via the comment parameter in the function FUN_00418c24.	9.8	More Details
CVE-2022-29391	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a stack overflow via the comment parameter in the function FUN_004200c8.	9.8	More Details
CVE-2022-1505	The RSVPMaker plugin for WordPress is vulnerable to unauthenticated SQL Injection due to missing SQL escaping and parameterization on user supplied data passed to a SQL query in the rsvpmaker-api-endpoints.php file. This makes it possible for unauthenticated attackers to steal sensitive information from the database in versions up to and including 9.2.6.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1453	The RSVPMaker plugin for WordPress is vulnerable to unauthenticated SQL Injection due to missing SQL escaping and parameterization on user supplied data passed to a SQL query in the rsvpmaker-util.php file. This makes it possible for unauthenticated attackers to steal sensitive information from the database in versions up to and including 9.2.5.	9.8	More Details
CVE-2022-23676	A remote execution of arbitrary code vulnerability was discovered in ArubaOS-Switch Devices version(s): ArubaOS-Switch 15.xx.xxxx: All versions; ArubaOS-Switch 16.01.xxxx: All versions; ArubaOS-Switch 16.02.xxxx: K.16.02.0033 and below; ArubaOS-Switch 16.03.xxxx: All versions; ArubaOS-Switch 16.04.xxxx: All versions; ArubaOS-Switch 16.05.xxxx: All versions; ArubaOS-Switch 16.06.xxxx: All versions; ArubaOS-Switch 16.07.xxxx: All versions; ArubaOS-Switch 16.08.xxxx: KB/WB/WC/YA/YB/YC.16.08.0024 and below; ArubaOS-Switch 16.09.xxxx: KB/WB/WC/YA/YB/YC.16.09.0019 and below; ArubaOS-Switch 16.10.xxxx: KB/WB/WC/YA/YB/YC.16.10.0019 and below; ArubaOS-Switch 16.11.xxxx: KB/WB/WC/YA/YB/YC.16.11.0003 and below. Aruba has released upgrades for ArubaOS-Switch Devices that address these security vulnerabilities.	9.8	More Details
CVE-2022-29329	D-Link DAP-1330_OSS-firmware_1.00b21 was discovered to contain a heap overflow via the devicename parameter in /goform/setDeviceSettings.	9.8	More Details
CVE-2022-29328	D-Link DAP-1330_OSS-firmware_1.00b21 was discovered to contain a stack overflow via the function checkvalidupgrade.	9.8	More Details
CVE-2022-29327	D-Link DIR-816 A2_v1.10CNB04 was discovered to contain a stack overflow via the urladd parameter in /goform/websURLFilterAddDel.	9.8	More Details
CVE-2022-29326	D-Link DIR-816 A2_v1.10CNB04 was discovered to contain a stack overflow via the addhostfilter parameter in /goform/websHostFilter.	9.8	More Details
CVE-2022-29325	D-Link DIR-816 A2_v1.10CNB04 was discovered to contain a stack overflow via the addurlfilter parameter in /goform/websURLFilter.	9.8	More Details
CVE-2022-29324	D-Link DIR-816 A2_v1.10CNB04 was discovered to contain a stack overflow via the proto parameter in /goform/form2IPQoSTcAdd.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29323	D-Link DIR-816 A2_v1.10CNB04 was discovered to contain a stack overflow via the MAC parameter in /goform/editassignment.	9.8	More Details
CVE-2022-0826	The WP Video Gallery WordPress plugin through 1.7.1 does not sanitise and escape a parameter before using it in a SQL statement via an AJAX action, leading to an SQL Injection exploitable by unauthenticated users	9.8	More Details
CVE-2022-0836	The SEMA API WordPress plugin before 4.02 does not properly sanitise and escape some parameters before using them in SQL statements via an AJAX action, leading to SQL Injections exploitable by unauthenticated users	9.8	More Details
CVE-2022-0592	The MapSVG WordPress plugin before 6.2.20 does not validate and escape a parameter via a REST endpoint before using it in a SQL statement, leading to a SQL Injection exploitable by unauthenticated users.	9.8	More Details
CVE-2022-0817	The BadgeOS WordPress plugin through 3.7.0 does not sanitise and escape a parameter before using it in a SQL statement via an AJAX action, leading to an SQL Injection exploitable by unauthenticated users	9.8	More Details
CVE-2022-29592	Tenda TX9 Pro 22.03.02.10 devices allow OS command injection via set_route (called by doSystemCmd_route).	9.8	More Details
CVE-2022-28606	An arbitrary file upload vulnerability exists in Wenzhou Huoyin Information Technology Co., Ltd. BossCMS 1.0, which can be exploited by an attacker to gain control of the server.	9.8	More Details
CVE-2022-28533	Sourcecodester Medical Hub Directory Site 1.0 is vulnerable to SQL Injection via /mhds/clinic/view_details.php.	9.8	More Details
CVE-2022-28530	Sourcecodester Covid-19 Directory on Vaccination System 1.0 is vulnerable to SQL Injection via cmdcategory.	9.8	More Details
CVE-2022-28120	Beijing Runnier Network Technology Co., Ltd Open virtual simulation experiment teaching management platform software 2.0 has a file upload vulnerability, which can be exploited by an attacker to gain control of the server.	9.8	More Details
CVE-2022-27588	We have already fixed this vulnerability in the following versions of QVR: QVR 5.1.6 build 20220401 and later	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1388	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	9.8	More Details
CVE-2022-28461	mingyuefusu Library Management System all versions as of 03-27-2022 is vulnerable to SQL Injection.	9.8	More Details
CVE-2021-42242	A command execution vulnerability exists in jfinal_cms 5.0.1 via com.jflyfox.component.controller.Ueditor.	9.8	More Details
CVE-2021-41739	A OS Command Injection vulnerability was discovered in Artica Proxy 4.30.000000. Attackers can execute OS commands in cyrus.events.php with GET param logs and POST param rp.	9.8	More Details
CVE-2022-28890	A vulnerability in the RDF/XML parser of Apache Jena allows an attacker to cause an external DTD to be retrieved. This issue affects Apache Jena version 4.4.0 and prior versions. Apache Jena 4.2.x and 4.3.x do not allow external entities.	9.8	More Details
CVE-2022-29155	In OpenLDAP 2.x before 2.5.12 and 2.6.x before 2.6.2, a SQL injection vulnerability exists in the experimental back-sql backend to slapd, via a SQL statement within an LDAP query. This can occur during an LDAP search operation when the search filter is processed, due to a lack of proper escaping.	9.8	More Details
CVE-2021-42235	SQL injection in osTicket before 1.14.8 and 1.15.4 login and password reset process allows attackers to access the osTicket administration profile functionality.	9.8	More Details
CVE-2022-28557	There is a command injection vulnerability at the /goform/setsambacfg interface of Tenda AC15 US_AC15V1.0BR_V15.03.05.20_multi_TDE01.bin device web, which can also cooperate with CVE-2021-44971 to cause unconditional arbitrary command execution	9.8	More Details
CVE-2022-29347	An arbitrary file upload vulnerability in Web@rchiv 1.0 allows attackers to execute arbitrary commands via a crafted PHP file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28568	Sourcecodester Doctor's Appointment System 1.0 is vulnerable to File Upload to RCE via Image upload from the administrator panel. An attacker can obtain remote command execution just by knowing the path where the images are stored.	9.8	More Details
CVE-2022-28512	A SQL injection vulnerability exists in Sourcecodester Fantastic Blog CMS 1.0 . An attacker can inject query in "/fantasticblog/single.php" via the "id=5" parameters.	9.8	More Details
CVE-2022-28082	Tenda AX12 v22.03.01.21_CN was discovered to contain a stack overflow via the list parameter at /goform/SetNetControlList.	9.8	More Details
CVE-2022-28111	MyBatis PageHelper v1.x.x-v3.7.0 v4.0.0-v5.0.0,v5.1.0-v5.3.0 was discovered to contain a time-blind SQL injection vulnerability via the orderBy parameter.	9.8	More Details
CVE-2021-42185	wdja v2.1 is affected by a SQL injection vulnerability in the foreground search function.	9.8	More Details
CVE-2022-28055	Fusionpbx v4.4 and below contains a command injection vulnerability via the download email logs function.	9.8	More Details
CVE-2022-27431	Wuzhicms v4.1.0 was discovered to contain a SQL injection vulnerability via the groupid parameter at /coreframe/app/member/admin/group.php.	9.8	More Details
CVE-2022-0814	The Ubigeo de Perú para Woocommerce WordPress plugin before 3.6.4 does not properly sanitise and escape some parameters before using them in SQL statements via various AJAX actions, some of which are available to unauthenticated users, leading to SQL Injections	9.8	More Details
CVE-2022-29502	SchedMD Slurm 21.08.x through 20.11.x has Incorrect Access Control that leads to Escalation of Privileges.	9.8	More Details
CVE-2022-28575	It is found that there is a command injection vulnerability in the setopenvpnclientcfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows attackers to execute arbitrary commands through a carefully constructed payload	9.8	More Details
CVE-2022-27411	TOTOLINK N600R v5.3c.5507_B20171031 was discovered to contain a command injection vulnerability via the QUERY_STRING parameter in the "Main" function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27420	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the patient_contact parameter in patientsearch.php.	9.8	More Details
CVE-2022-28470	marcador package in PyPI 0.1 through 0.13 included a code-execution backdoor.	9.8	More Details
CVE-2019-12254	In multiple Tecson Tankspion and GOKs SmartBox 4 products the affected application doesn't properly restrict access to an endpoint that is responsible for saving settings, to a unauthenticated user with limited access rights. Based on the lack of adequately implemented access-control rules, by accessing a specific uniform resource locator (URL) on the web server, a malicious user is able to change the application settings without authenticating at all, which violates originally laid ACL rules.	9.8	More Details
CVE-2022-28163	In Brocade SANnav before Brocade SANnav 2.2.0, multiple endpoints associated with Zone management are susceptible to SQL injection, allowing an attacker to run arbitrary SQL commands.	9.8	More Details
CVE-2022-28005	An issue was discovered in the 3CX Phone System Management Console prior to version 18 Update 3 FINAL. An unauthenticated attacker could abuse improperly secured access to arbitrary files on the server (via /Electron/download directory traversal in conjunction with a path component that uses backslash characters), leading to cleartext credential disclosure. Afterwards, the authenticated attacker is able to upload a file that overwrites a 3CX service binary, leading to Remote Code Execution as NT AUTHORITY\SYSTEM on Windows installations. NOTE: this issue exists because of an incomplete fix for CVE-2022-48482.	9.8	More Details
CVE-2020-19213	SQL Injection vulnerability in cat_move.php in piwigo v2.9.5, via the selection parameter to move_categories.	9.8	More Details
CVE-2022-28577	It is found that there is a command injection vulnerability in the delParentalRules interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.	9.8	More Details
CVE-2022-29535	Zoho ManageEngine OPManager through 125588 allows SQL Injection via a few default reports.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29130	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	9.8	More Details
CVE-2022-28578	It is found that there is a command injection vulnerability in the setOpenVpnCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.	9.8	More Details
CVE-2022-27360	SpringBlade v3.2.0 and below was discovered to contain a SQL injection vulnerability via the component customSqlSegment.	9.8	More Details
CVE-2022-28584	It is found that there is a command injection vulnerability in the setWiFiWpsStart interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.	9.8	More Details
CVE-2022-28583	It is found that there is a command injection vulnerability in the setWiFiWpsCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.	9.8	More Details
CVE-2022-28582	It is found that there is a command injection vulnerability in the setWiFiSignalCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.	9.8	More Details
CVE-2022-28581	It is found that there is a command injection vulnerability in the setWiFiAdvancedCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.	9.8	More Details
CVE-2022-28580	It is found that there is a command injection vulnerability in the setL2tpServerCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.	9.8	More Details
CVE-2022-28579	It is found that there is a command injection vulnerability in the setParentalRules interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.	9.8	More Details
CVE-2022-1575	Arbitrary Code Execution through Sanitizer Bypass in GitHub repository jgraph/drawio prior to 18.0.0. - Arbitrary (remote) code execution in the desktop app. - Stored XSS in the web app.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24042	A vulnerability has been identified in Desigo DXR2 (All versions < V01.21.142.5-22), Desigo PXC3 (All versions < V01.21.142.4-18), Desigo PXC4 (All versions < V02.20.142.10-10884), Desigo PXC5 (All versions < V02.20.142.10-10884). The web application returns an AuthToken that does not expire at the defined auto logoff delay timeout. An attacker could be able to capture this token and re-use old session credentials or session IDs for authorization.	9.1	More Details
CVE-2021-42581	Prototype poisoning in function mapObjIndexed in Ramda 0.27.0 and earlier allows attackers to compromise integrity or availability of application via supplying a crafted object (that contains an own property "__proto__") as an argument to the function. NOTE: the vendor disputes this because the observed behavior only means that a user can create objects that the user didn't know would contain custom prototypes	9.1	More Details
CVE-2022-1053	Keylime does not enforce that the agent registrar data is the same when the tenant uses it for validation of the EK and identity quote and the verifier for validating the integrity quote. This allows an attacker to use one AK, EK pair from a real TPM to pass EK validation and give the verifier an AK of a software TPM. A successful attack breaks the entire chain of trust because a not validated AK is used by the verifier. This issue is worse if the validation happens first and then the agent gets added to the verifier because the timing is easier and the verifier does not validate the regcount entry being equal to 1,	9.1	More Details
CVE-2022-25784	Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7.	9.1	More Details
CVE-2022-23066	In Solana rBPF versions 0.2.26 and 0.2.27 are affected by Incorrect Calculation which is caused by improper implementation of sdiv instruction. This can lead to the wrong execution path, resulting in huge loss in specific cases. For example, the result of a sdiv instruction may decide whether to transfer tokens or not. The vulnerability affects both integrity and may cause serious availability problems.	9.1	More Details
CVE-2022-0947	A vulnerability in ABB ARG600 Wireless Gateway series that could allow an attacker to exploit the vulnerability by remotely connecting to the serial port gateway, and/or protocol converter, depending on the configuration.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24039	A vulnerability has been identified in Desigo PXC4 (All versions < V02.20.142.10-10884), Desigo PXC5 (All versions < V02.20.142.10-10884). The “addCell” JavaScript function fails to properly sanitize user-controllable input before including it into the generated XML body of the XLS report document, such that it is possible to inject arbitrary content (e.g., XML tags) into the generated file. An attacker with restricted privileges, by poisoning any of the content used to generate XLS reports, could be able to leverage the application to deliver malicious files against higher-privileged users and obtain Remote Code Execution (RCE) against the administrator’s workstation.	9.0	More Details
CVE-2022-30284	In the python-libnmap package through 0.7.2 for Python, remote command execution can occur (if used in a client application that does not validate arguments). NOTE: the vendor believes it would be unrealistic for an application to call NmapProcess with arguments taken from input data that arrived over an untrusted network, and thus the CVSS score corresponds to an unrealistic use case. None of the NmapProcess documentation implies that this is an expected use case	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-43159	A Remote Code Execution (RCE) vulnerability exists in Ruijie Networks Ruijie RG-EW Series Routers up to ReyeeOS 1.55.1915 / EW_3.0(1)B11P55 via the setSessionTime function in /cgi-bin/luci/api/common..	8.8	More Details
CVE-2020-19216	SQL Injection vulnerability in admin/user_perm.php in piwigo v2.9.5, via the cat_false parameter to admin.php?page=group_perm.	8.8	More Details
CVE-2022-29141	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-43160	A Remote Code Execution (RCE) vulnerability exists in Ruijie Networks Ruijie RG-EW Series Routers up to ReyeeOS 1.55.1915 / EW_3.0(1)B11P55 via the switchFastDhcp function in /cgi-bin/luci/api/diagnose.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28165	A vulnerability in the role-based access control (RBAC) functionality of the Brocade SANNav before 2.2.0 could allow an authenticated, remote attacker to access resources that they should not be able to access and perform actions that they should not be able to perform. The vulnerability exists because restrictions are not performed on Server side to ensure the user has required permission before processing requests.	8.8	More Details
CVE-2022-27183	The Monitoring Console app configured in Distributed mode allows for a Reflected XSS in a query parameter in Splunk Enterprise versions before 8.1.4. The Monitoring Console app is a bundled app included in Splunk Enterprise, not for download on SplunkBase, and not installed on Splunk Cloud Platform instances. Note that the Cloud Monitoring Console is not impacted.	8.8	More Details
CVE-2022-26889	In Splunk Enterprise versions before 8.1.2, the uri path to load a relative resource within a web page is vulnerable to path traversal. It allows an attacker to potentially inject arbitrary content into the web page (e.g., HTML Injection, XSS) or bypass SPL safeguards for risky commands. The attack is browser-based. An attacker cannot exploit the attack at will and requires the attacker to initiate a request within the victim's browser (e.g., phishing).	8.8	More Details
CVE-2020-19217	SQL Injection vulnerability in admin/batch_manager.php in piwigo v2.9.5, via the filter_category parameter to admin.php?page=batch_manager.	8.8	More Details
CVE-2020-19215	SQL Injection vulnerability in admin/user_perm.php in piwigo v2.9.5, via the cat_false parameter to admin.php?page=user_perm.	8.8	More Details
CVE-2022-29137	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-25989	An authentication bypass vulnerability exists in the libxm_av.so getpeermac() functionality of Anker Eufy Homebase 2 2.1.8.5h. A specially-crafted DHCP packet can lead to authentication bypass. An attacker can DHCP poison to trigger this vulnerability.	8.8	More Details
CVE-2022-29501	SchedMD Slurm 21.08.x through 20.11.x has Incorrect Access Control that leads to Escalation of Privileges and code execution.	8.8	More Details
CVE-2022-29500	SchedMD Slurm 21.08.x through 20.11.x has Incorrect Access Control that leads to Information Disclosure.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28080	Royal Event Management System v1.0 was discovered to contain a SQL injection vulnerability via the todate parameter.	8.8	More Details
CVE-2022-28079	College Management System v1.0 was discovered to contain a SQL injection vulnerability via the course_code parameter.	8.8	More Details
CVE-2021-44051	A command injection vulnerability has been reported to affect QNAP NAS running QuTScloud, QuTS hero and QTS. If exploited, this vulnerability allows remote attackers to run arbitrary commands. We have already fixed this vulnerability in the following versions of QuTScloud, QuTS hero and QTS: QuTScloud c5.0.1.1949 and later QuTS hero h5.0.0.1986 build 20220324 and later QTS 5.0.0.1986 build 20220324 and later	8.8	More Details
CVE-2022-29139	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-29133	Windows Kernel Elevation of Privilege Vulnerability	8.8	More Details
CVE-2021-41020	An improper access control vulnerability [CWE-284] in FortiIsolator versions 2.3.2 and below may allow an authenticated, non privileged attacker to regenerate the CA certificate via the regeneration URL.	8.8	More Details
CVE-2022-22013	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-29108	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-26927	Windows Graphics Component Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-26923	Active Directory Domain Services Elevation of Privilege Vulnerability	8.8	More Details
CVE-2022-22019	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22017	Remote Desktop Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-22014	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-1463	The Booking Calendar plugin for WordPress is vulnerable to PHP Object Injection via the [bookingflextimeline] shortcode in versions up to, and including, 9.1. This could be exploited by subscriber-level users and above to call arbitrary PHP objects on a vulnerable site.	8.8	More Details
CVE-2022-29131	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-1397	API Privilege Escalation in GitHub repository alextselegidis/easyappointments prior to 1.5.0. Full system takeover.	8.8	More Details
CVE-2022-29933	Craft CMS through 3.7.36 allows a remote unauthenticated attacker, who knows at least one valid username, to reset the account's password and take over the account by providing a crafted HTTP header to the application while using the password reset functionality. Specifically, the attacker must send X-Forwarded-Host to the /index.php?p=admin/actions/users/send-password-reset-email URI. NOTE: the vendor's position is that a customer can already work around this by adjusting the configuration (i.e., by not using the default configuration).	8.8	More Details
CVE-2022-23332	Command injection vulnerability in Manual Ping Form (Web UI) in Shenzhen Ejoin Information Technology Co., Ltd. ACOM508/ACOM516/ACOM532 609-915-041-100-020 allows a remote attacker to inject arbitrary code via the field.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1631	Users Account Pre-Takeover or Users Account Takeover. in GitHub repository microweber/microweber prior to 1.2.15. Victim Account Take Over. Since, there is no email confirmation, an attacker can easily create an account in the application using the Victim's Email. This allows an attacker to gain pre-authentication to the victim's account. Further, due to the lack of proper validation of email coming from Social Login and failing to check if an account already exists, the victim will not identify if an account is already existing. Hence, the attacker's persistence will remain. An attacker would be able to see all the activities performed by the victim user impacting the confidentiality and attempt to modify/corrupt the data impacting the integrity and availability factor. This attack becomes more interesting when an attacker can register an account from an employee's email address. Assuming the organization uses G-Suite, it is much more impactful to hijack into an employee's account.	8.8	More Details
CVE-2022-29128	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-29129	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-29938	In LibreHealth EHR 2.0.0, lack of sanitization of the GET parameter payment_id in interface\billing\new_payment.php via interface\billing\payment_master.inc.php leads to SQL injection.	8.8	More Details
CVE-2021-42743	A misconfiguration in the node default path allows for local privilege escalation from a lower privileged user to the Splunk user in Splunk Enterprise versions before 8.1.1 on Windows.	8.8	More Details
CVE-2021-43162	A Remote Code Execution (RCE) vulnerability exists in Ruijie Networks Ruijie RG-EW Series Routers up to ReyeeOS 1.55.1915 / EW_3.0(1)B11P55 via the runPackDiagnose function in /cgi-bin/luci/api/diagnose.	8.8	More Details
CVE-2022-30129	Visual Studio Code Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-27903	An OS Command Injection vulnerability in the configuration parser of Eve-NG Professional through 4.0.1-65 and Eve-NG Community through 2.0.3-112 allows a remote authenticated attacker to execute commands as root by editing virtualization command parameters of imported UNL files.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28099	Poultry Farm Management System v1.0 was discovered to contain a SQL injection vulnerability via the Item parameter at /farm/store.php.	8.8	More Details
CVE-2022-28552	Cscms 4.1 is vulnerable to SQL Injection. Log into the background, open the song module, create a new song, delete it to the recycle bin, and SQL injection security problems will occur when emptying the recycle bin.	8.8	More Details
CVE-2021-42192	Konga v0.14.9 is affected by an incorrect access control vulnerability where a specially crafted request can lead to privilege escalation.	8.8	More Details
CVE-2021-43161	A Remote Code Execution (RCE) vulnerability exists in Ruijie Networks Ruijie RG-EW Series Routers up to ReyeeOS 1.55.1915 / EW_3.0(1)B11P55 via the doSwitchApi function in /cgi-bin/luci/api/switch.	8.8	More Details
CVE-2021-43164	A Remote Code Execution (RCE) vulnerability exists in Ruijie Networks Ruijie RG-EW Series Routers up to ReyeeOS 1.55.1915 / EW_3.0(1)B11P55 via the updateVersion function in /cgi-bin/luci/api/wireless.	8.8	More Details
CVE-2022-27806	On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP Advanced WAF, ASM, and ASM, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, when running in Appliance mode, an authenticated attacker assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing command injection vulnerabilities in undisclosed URIs in F5 BIG-IP Guided Configuration. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	8.7	More Details
CVE-2022-25946	On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP Advanced WAF, ASM, and ASM, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, when running in Appliance mode, an authenticated attacker with Administrator role privilege may be able to bypass Appliance mode restrictions due to a missing integrity check in F5 BIG-IP Guided Configuration. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22774	The DOM XML parser and SAX XML parser components of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center, TIBCO Managed File Transfer Command Center, TIBCO Managed File Transfer Internet Server, and TIBCO Managed File Transfer Internet Server contains an easily exploitable vulnerability that allows an unauthenticated attacker with network access to execute XML External Entity (XXE) attacks on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions 8.3.1 and below, TIBCO Managed File Transfer Command Center: versions 8.4.0 and 8.4.1, TIBCO Managed File Transfer Internet Server: versions 8.3.1 and below, and TIBCO Managed File Transfer Internet Server: versions 8.4.0 and 8.4.1.	8.6	More Details
CVE-2021-38447	OCI OpenDDS versions prior to 3.18.1 are vulnerable when an attacker sends a specially crafted packet to flood target devices with unwanted traffic, which may result in a denial-of-service condition.	8.6	More Details
CVE-2022-20770	On April 20, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in CHM file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog. This advisory will be updated as additional information becomes available.	8.6	More Details
CVE-2021-38439	All versions of GurumDDS are vulnerable to heap-based buffer overflow, which may cause a denial-of-service condition or remotely execute arbitrary code.	8.6	More Details
CVE-2022-28067	An incorrect access control issue in Sandboxie Classic v5.55.13 allows attackers to cause a Denial of Service (DoS) in the Sandbox via a crafted executable.	8.6	More Details
CVE-2021-25268	Multiple XSS vulnerabilities in Webadmin allow for privilege escalation from MySophos admin to SFOS admin in Sophos Firewall older than version 19.0 GA.	8.4	More Details
CVE-2022-26932	Storage Spaces Direct Elevation of Privilege Vulnerability	8.2	More Details
CVE-2022-1592	Server-Side Request Forgery in scout in GitHub repository clinical-genomics/scout prior to v4.42. An attacker could make the application perform arbitrary requests to fishing steal cookie, request to private area, or lead to xss...	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21978	Microsoft Exchange Server Elevation of Privilege Vulnerability	8.2	More Details
CVE-2022-21972	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-23677	A remote execution of arbitrary code vulnerability was discovered in ArubaOS-Switch Devices version(s): ArubaOS-Switch 15.xx.xxxx: All versions; ArubaOS-Switch 16.01.xxxx: All versions; ArubaOS-Switch 16.02.xxxx: K.16.02.0033 and below; ArubaOS-Switch 16.03.xxxx: All versions; ArubaOS-Switch 16.04.xxxx: All versions; ArubaOS-Switch 16.05.xxxx: All versions; ArubaOS-Switch 16.06.xxxx: All versions; ArubaOS-Switch 16.07.xxxx: All versions; ArubaOS-Switch 16.08.xxxx: KB/WB/WC/YA/YB/YC.16.08.0024 and below; ArubaOS-Switch 16.09.xxxx: KB/WB/WC/YA/YB/YC.16.09.0019 and below; ArubaOS-Switch 16.10.xxxx: KB/WB/WC/YA/YB/YC.16.10.0019 and below; ArubaOS-Switch 16.11.xxxx: KB/WB/WC/YA/YB/YC.16.11.0003 and below. Aruba has released upgrades for ArubaOS-Switch Devices that address these security vulnerabilities.	8.1	More Details
CVE-2022-24903	Rsyslog is a rocket-fast system for log processing. Modules for TCP syslog reception have a potential heap buffer overflow when octet-counted framing is used. This can result in a segfault or some other malfunction. As of our understanding, this vulnerability can not be used for remote code execution. But there may still be a slight chance for experts to do that. The bug occurs when the octet count is read. While there is a check for the maximum number of octets, digits are written to a heap buffer even when the octet count is over the maximum, This can be used to overrun the memory buffer. However, once the sequence of digits stop, no additional characters can be added to the buffer. In our opinion, this makes remote exploits impossible or at least highly complex. Octet-counted framing is one of two potential framing modes. It is relatively uncommon, but enabled by default on receivers. Modules `imtcp`, `imptcp`, `imgssapi`, and `imhttp` are used for regular syslog message reception. It is best practice not to directly expose them to the public. When this practice is followed, the risk is considerably lower. Module `imdiag` is a diagnostics module primarily intended for testbench runs. We do not expect it to be present on any production installation. Octet-counted framing is not very common. Usually, it needs to be specifically enabled at senders. If users do not need it, they can turn it off for the most important modules. This will mitigate the vulnerability.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-25033	ADMesh through 0.98.4 has a heap-based buffer over-read in stl_update_connects_remove_1 (called from stl_remove_degenerate) in connect.c in libadmesh.a.	8.1	More Details
CVE-2022-23270	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-26925	Windows LSA Spoofing Vulnerability	8.1	More Details
CVE-2021-26253	A potential vulnerability in Splunk Enterprise's implementation of DUO MFA allows for bypassing the MFA verification in Splunk Enterprise versions before 8.1.6. The potential vulnerability impacts Splunk Enterprise instances configured to use DUO MFA and does not impact or affect a DUO product or service.	8.1	More Details
CVE-2022-28707	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility (also referred to as the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	8.0	More Details
CVE-2022-21934	Under certain circumstances an authenticated user could lock other users out of the system or take over their accounts in Metasys ADS/ADX/OAS server 10 versions prior to 10.1.5 and Metasys ADS/ADX/OAS server 11 versions prior to 11.0.2.	8.0	More Details
CVE-2022-29166	matrix-appservice-irc is a Node.js IRC bridge for Matrix. The vulnerability in node-irc allows an attacker to manipulate a Matrix user into executing IRC commands by having them reply to a maliciously crafted message. The vulnerability has been patched in matrix-appservice-irc 0.33.2. Refrain from replying to messages from untrusted participants in IRC-bridged Matrix rooms. There are no known workarounds for this issue.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29173	go-tuf is a Go implementation of The Update Framework (TUF). go-tuf does not correctly implement the client workflow for updating the metadata files for roles other than the root role. Specifically, checks for rollback attacks are not implemented correctly meaning an attacker can cause clients to install software that is older than the software which the client previously knew to be available, and may include software with known vulnerabilities. In more detail, the client code of go-tuf has several issues in regards to preventing rollback attacks: 1. It does not take into account the content of any previously trusted metadata, if available, before proceeding with updating roles other than the root role (i.e., steps 5.4.3.1 and 5.5.5 of the detailed client workflow). This means that any form of version verification done on the newly-downloaded metadata is made using the default value of zero, which always passes. 2. For both timestamp and snapshot roles, go-tuf saves these metadata files as trusted before verifying if the version of the metafiles they refer to is correct (i.e., steps 5.5.4 and 5.6.4 of the detailed client workflow). A fix is available in version 0.3.0 or newer. No workarounds are known for this issue apart from upgrading.	8.0	More Details
CVE-2022-29148	Visual Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-30240	An argument injection vulnerability in the browser-based authentication component of the Magnitude Simba Amazon Redshift JDBC Driver 1.2.40 through 1.2.55 may allow a local user to execute code. NOTE: this is different from CVE-2022-29972.	7.8	More Details
CVE-2022-30239	An argument injection vulnerability in the browser-based authentication component of the Magnitude Simba Amazon Athena JDBC Driver 2.0.25 through 2.0.28 may allow a local user to execute code. NOTE: this is different from CVE-2022-29971.	7.8	More Details
CVE-2022-20005	In validateApkInstallLocked of PackageInstallerSession.java, there is a way to force a mismatch between running code and a parsed APK . This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-219044664	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29263	On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, as well as F5 BIG-IP APM Clients 7.x versions prior to 7.2.1.5, the BIG-IP Edge Client Component Installer Service does not use best practice while saving temporary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.8	More Details
CVE-2022-28806	An issue was discovered on certain Fujitsu LIEFBOOK devices (A3510, U9310, U7511/U7411/U7311, U9311, E5510/E5410, U7510/U7410/U7310, E459/E449) with BIOS versions before v1.09 (A3510), v2.17 (U9310), v2.30 (U7511/U7411/U7311), v2.33 (U9311), v2.23 (E5510), v2.19 (U7510/U7410), v2.13 (U7310), and v1.09 (E459/E449). The FjGabiFlashCoreAbstractionSmm driver registers a Software System Management Interrupt (SWSMI) handler that is not sufficiently validated to ensure that the CommBuffer (or any other communication buffer's nested contents) are not pointing to SMRAM contents. A potential attacker can therefore write fixed data to SMRAM, which could lead to data corruption inside this memory (e.g., change the SMI handler's code or modify SMRAM map structures to break input pointer validation for other SMI handlers). Thus, the attacker could elevate privileges from ring 0 to ring -2 and execute arbitrary code in SMM.	7.8	More Details
CVE-2022-20004	In checkSlicePermission of SliceManagerService.java, it is possible to access any slice URI due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-179699767	7.8	More Details
CVE-2022-29972	An argument injection vulnerability in the browser-based authentication component of the Magnitude Simba Amazon Redshift ODBC Driver (1.4.14 through 1.4.21.1001 and 1.4.22 through 1.4.x before 1.4.52) may allow a local user to execute arbitrary code.	7.8	More Details
CVE-2022-29971	An argument injection vulnerability in the browser-based authentication component of the Magnitude Simba Amazon Athena ODBC Driver 1.1.1 through 1.1.x before 1.1.17 may allow a local user to execute arbitrary code.	7.8	More Details
CVE-2022-1616	Use after free in append_command in GitHub repository vim/vim prior to 8.2.4895. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1621	Heap buffer overflow in vim_strncpy find_word in GitHub repository vim/vim prior to 8.2.4919. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution	7.8	More Details
CVE-2021-26324	A bug with the SEV-ES TMR may lead to a potential loss of memory integrity for SNP-active VMs.	7.8	More Details
CVE-2022-1629	Buffer Over-read in function find_next_quote in GitHub repository vim/vim prior to 8.2.4925. This vulnerabilities are capable of crashing software, Modify Memory, and possible remote execution	7.8	More Details
CVE-2022-26987	TP-Link TL-WDR7660 2.0.30, Mercury D196G 20200109_2.0.4, and Fast FAC1900R 20190827_2.0.2 routers have a stack overflow issue in `MmtAtePrase` function. Local users could get remote code execution.	7.8	More Details
CVE-2021-46771	Insufficient validation of addresses in AMD Secure Processor (ASP) firmware system call may potentially lead to arbitrary code execution by a compromised user application.	7.8	More Details
CVE-2022-26988	TP-Link TL-WDR7660 2.0.30, Mercury D196G 20200109_2.0.4, and Fast FAC1900R 20190827_2.0.2 routers have a stack overflow issue in `MntAte` function. Local users could get remote code execution.	7.8	More Details
CVE-2022-28463	ImageMagick 7.1.0-27 is vulnerable to Buffer Overflow.	7.8	More Details
CVE-2021-26353	Failure to validate inputs in SMM may allow an attacker to create a mishandled error leaving the DRTM UApp in a partially initialized state potentially resulting in loss of memory integrity.	7.8	More Details
CVE-2022-22454	IBM InfoSphere Information Server 11.7 could allow a locally authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request.	7.8	More Details
CVE-2022-1619	Heap-based Buffer Overflow in function cmdline_erase_chars in GitHub repository vim/vim prior to 8.2.4899. This vulnerabilities are capable of crashing software, modify memory, and possible remote execution	7.8	More Details
CVE-2021-20051	SonicWall Global VPN Client 4.10.7.1117 installer (32-bit and 64-bit) and earlier versions have a DLL Search Order Hijacking vulnerability in one of the installer components. Successful exploitation via a local attacker could result in command execution in the target system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20114	In placeCall of TelecomManager.java, there is a possible way for an application to keep itself running with foreground service importance due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-211114016	7.8	More Details
CVE-2022-20113	In mPreference of DefaultUsbConfigurationPreferenceController.java, there is a possible way to enable file transfer mode due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-205996517	7.8	More Details
CVE-2022-26926	Windows Address Book Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-27784	Adobe After Effects versions 22.2.1 (and earlier) and 18.4.5 (and earlier) are affected by a stack overflow vulnerability due to insecure handling of a crafted 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 file in After Effects.	7.8	More Details
CVE-2022-29103	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-29104	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-29105	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-29109	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-27783	Adobe After Effects versions 22.2.1 (and earlier) and 18.4.5 (and earlier) are affected by a stack overflow vulnerability due to insecure handling of a crafted 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 file in After Effects.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29132	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-28278	Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-27470	SDL_ttf v2.0.18 and below was discovered to contain an arbitrary memory write via the function TTF_RenderText_Solid(). This vulnerability is triggered via a crafted TTF file.	7.8	More Details
CVE-2022-24098	Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are affected by an improper input validation vulnerability when parsing a PCX file 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 PCX file.	7.8	More Details
CVE-2022-29110	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-29113	Windows Digital Media Receiver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-39738	In CarSetings, there is a possible to pair BT device bypassing user's consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-216190509	7.8	More Details
CVE-2022-29115	Windows Fax Service Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-20116	In onEntryUpdated of OngoingCallController.kt, it is possible to launch non-exported activities due to intent redirection. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-212467440	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30524	There is an invalid memory access in the TextLine class in TextOutputDev.cc in Xpdf 4.0.4 because the text extractor mishandles characters at large y coordinates. It can be triggered by (for example) sending a crafted pdf file to the pdftotext binary, which allows a remote attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact.	7.8	More Details
CVE-2021-23592	The package topthink/framework before 6.0.12 are vulnerable to Deserialization of Untrusted Data due to insecure unserialize method in the Driver class.	7.7	More Details
CVE-2022-24878	Flux is an open and extensible continuous delivery solution for Kubernetes. Path Traversal in the kustomize-controller via a malicious `kustomization.yaml` allows an attacker to cause a Denial of Service at the controller level. Workarounds include automated tooling in the user's CI/CD pipeline to validate `kustomization.yaml` files conform with specific policies. This vulnerability is fixed in kustomize-controller v0.24.0 and included in flux2 v0.29.0. Users are recommended to upgrade.	7.7	More Details
CVE-2022-26415	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.7	More Details
CVE-2021-25745	A security issue was discovered in ingress-nginx where a user that can create or update ingress objects can use the spec.rules[].http.paths[].path field of an Ingress object (in the networking.k8s.io or extensions API group) to obtain the credentials of the ingress-nginx controller. In the default configuration, that credential has access to all secrets in the cluster.	7.6	More Details
CVE-2021-25746	A security issue was discovered in ingress-nginx where a user that can create or update ingress objects can use .metadata.annotations in an Ingress object (in the networking.k8s.io or extensions API group) to obtain the credentials of the ingress-nginx controller. In the default configuration, that credential has access to all secrets in the cluster.	7.6	More Details
CVE-2022-30286	pyscriptjs (aka PyScript Demonstrator) in PyScript through 2022-05-04 allows a remote user to read Python source code.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28969	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the shareSpeed parameter in the function fromSetWifiGusetBasic. This vulnerability allows attackers to cause a Denial of Service (DoS).	7.5	More Details
CVE-2022-25787	Information Exposure Through Query Strings in GET Request vulnerability in LMM API of Secomea GateManager allows system administrator to hijack connection. This issue affects: Secomea GateManager all versions prior to 9.7.	7.5	More Details
CVE-2022-28716	On 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x 11.6.x, a DOM-based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP AFM, CGNAT, and PEM Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.5	More Details
CVE-2022-23802	Joomla Guru extension 5.2.5 is affected by: Insecure Permissions. The impact is: obtain sensitive information (remote). The component is: Access to private information and components, possibility to view other users' information. Information disclosure Access to private information and components, possibility to view other users' information.	7.5	More Details
CVE-2022-30293	In WebKitGTK through 2.36.0 (and WPE WebKit), there is a heap-based buffer overflow in WebCore::TextureMapperLayer::setContentsLayer in WebCore/platform/graphics/texmap/TextureMapperLayer.cpp.	7.5	More Details
CVE-2022-29145	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2022-25324	All versions of package bignum are vulnerable to Denial of Service (DoS) due to a type-check exception in V8, when verifying the type of the second argument to the .powm function, V8 will crash regardless of Node try/catch blocks.	7.5	More Details
CVE-2022-28739	There is a buffer over-read in Ruby before 2.6.10, 2.7.x before 2.7.6, 3.x before 3.0.4, and 3.1.x before 3.1.2. It occurs in String-to-Float conversion, including Kernel#Float and String#to_f.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29491	On F5 BIG-IP LTM, Advanced WAF, ASM, or APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and all versions of 13.1.x, 12.1.x, and 11.6.x, when a virtual server is configured with HTTP, TCP on one side (client/server), and DTLS on the other (server/client), undisclosed requests can cause the TMM process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.5	More Details
CVE-2021-20479	IBM Cloud Pak System 2.3.0 through 2.3.3.3 Interim Fix 1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 197498.	7.5	More Details
CVE-2022-28970	Tenda AX1806 v1.0.0.1 was discovered to contain a heap overflow via the mac parameter in the function GetParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS).	7.5	More Details
CVE-2021-31559	A crafted request bypasses S2S TCP Token authentication writing arbitrary events to an index in Splunk Enterprise Indexer 8.1 versions before 8.1.5 and 8.2 versions before 8.2.1. The vulnerability impacts Indexers configured to use TCPTokens. It does not impact Universal Forwarders.	7.5	More Details
CVE-2022-1620	NULL Pointer Dereference in function vim_regexec_string at regexp.c:2729 in GitHub repository vim/vim prior to 8.2.4901. NULL Pointer Dereference in function vim_regexec_string at regexp.c:2729 allows attackers to cause a denial of service (application crash) via a crafted input.	7.5	More Details
CVE-2022-28971	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the list parameter in the function fromSetIpMacBind. This vulnerability allows attackers to cause a Denial of Service (DoS).	7.5	More Details
CVE-2022-28487	Tcpreplay version 4.4.1 contains a memory leakage flaw in fix_ipv6_checksums() function. The highest threat from this vulnerability is to data confidentiality.	7.5	More Details
CVE-2022-30333	RARLAB UnRAR before 6.12 on Linux and UNIX allows directory traversal to write to files during an extract (aka unpack) operation, as demonstrated by creating a ~/.ssh/authorized_keys file. NOTE: WinRAR and Android RAR are unaffected.	7.5	More Details
CVE-2022-28972	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the timeZone parameter in the function form_fast_setting_wifi_set. This vulnerability allows attackers to cause a Denial of Service (DoS).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39023	IBM Guardium Data Encryption (GDE) 4.0.0 and 5.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 213860.	7.5	More Details
CVE-2022-28973	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the wanMTU parameter in the function fromAdvSetMacMtuWan. This vulnerability allows attackers to cause a Denial of Service (DoS).	7.5	More Details
CVE-2022-27189	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.5	More Details
CVE-2022-28705	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.5	More Details
CVE-2021-38425	eProsima Fast DDS versions prior to 2.4.0 (#2269) are susceptible to exploitation when an attacker sends a specially crafted packet to flood a target device with unwanted traffic, which may result in a denial-of-service condition and information exposure.	7.5	More Details
CVE-2022-28701	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.5	More Details
CVE-2022-24901	Improper validation of the Apple certificate URL in the Apple Game Center authentication adapter allows attackers to bypass authentication, making the server vulnerable to DoS attacks. The vulnerability has been fixed by improving the URL validation and adding additional checks of the resource the URL points to before downloading it.	7.5	More Details
CVE-2021-42183	MasaCMS 7.2.1 is affected by a path traversal vulnerability in /index.cfm/_api/asset/image/.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38487	RTI Connext DDS Professional, Connext DDS Secure versions 4.2x to 6.1.0, and Connext DDS Micro versions 2.4 and later are vulnerable when an attacker sends a specially crafted packet to flood target devices with unwanted traffic. This may result in a denial-of-service condition and information exposure.	7.5	More Details
CVE-2021-43547	TwinOaks Computing CoreDX DDS versions prior to 5.9.1 are susceptible to exploitation when an attacker sends a specially crafted packet to flood target devices with unwanted traffic. This may result in a denial-of-service condition and information exposure.	7.5	More Details
CVE-2022-1442	The Metform WordPress plugin is vulnerable to sensitive information disclosure due to improper access control in the ~/core/forms/action.php file which can be exploited by an unauthenticated attacker to view all API keys and secrets of integrated third-party APIs like that of PayPal, Stripe, Mailchimp, Hubspot, HelpScout, reCAPTCHA and many more, in versions up to and including 2.1.3.	7.5	More Details
CVE-2022-29340	GPAC 2.1-DEV-rev87-g053aae8-master. has a Null Pointer Dereference vulnerability in gf_isom_parse_movie_boxes_internal due to improper return value handling of GF_SKIP_BOX, which causes a Denial of Service. This vulnerability was fixed in commit 37592ad.	7.5	More Details
CVE-2022-28986	LMS Doctor Simple 2 Factor Authentication Plugin For Moodle Affected: 2021072900 has an Insecure direct object references (IDOR) vulnerability, which allows remote attackers to update sensitive records such as email, password and phone number of other user accounts.	7.5	More Details
CVE-2022-29339	In GPAC 2.1-DEV-rev87-g053aae8-master, function BS_ReadByte() in utils/bitstream.c has a failed assertion, which causes a Denial of Service. This vulnerability was fixed in commit 9ea93a2.	7.5	More Details
CVE-2022-23267	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2022-28462	novel-plus 3.6.0 suffers from an Arbitrary file reading vulnerability.	7.5	More Details
CVE-2021-43010	In Safedog Apache v4.0.30255, attackers can bypass this product for SQL injection. Attackers can bypass access to sensitive data.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30288	Agoo before 2.14.3 does not reject GraphQL fragment spreads that form cycles, leading to an application crash. NOTE: the vendor has disputed this on the grounds that it is not the server's responsibility to "enforce all the various ways a developer could write code with logic errors.	7.5	More Details
CVE-2022-26931	Windows Kerberos Elevation of Privilege Vulnerability	7.5	More Details
CVE-2022-26372	On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2022-20785	On April 20, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in HTML file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog. This advisory will be updated as additional information becomes available.	7.5	More Details
CVE-2022-20771	On April 20, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in the TIFF file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog. This advisory will be updated as additional information becomes available.	7.5	More Details
CVE-2022-26890	On F5 BIG-IP Advanced WAF, ASM, and APM 16.1.x versions prior to 16.1.2.1, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when ASM or Advanced WAF, as well as APM, are configured on a virtual server, the ASM policy is configured with Session Awareness, and the "Use APM Username and Session ID" option is enabled, undisclosed requests can cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27230	On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP APM, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of F5 BIG-IP Guided Configuration that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.5	More Details
CVE-2022-28940	In H3C MagicR100 <=V100R005, the / Ajax / ajaxget interface can be accessed without authorization. It sends a large amount of data through ajaxmsg to carry out DOS attack.	7.5	More Details
CVE-2021-41545	A vulnerability has been identified in Desigo DXR2 (All versions < V01.21.142.5-22), Desigo PXC3 (All versions < V01.21.142.4-18), Desigo PXC4 (All versions < V02.20.142.10-10884), Desigo PXC5 (All versions < V02.20.142.10-10884). When the controller receives a specific BACnet protocol packet, an exception causes the BACnet communication function to go into a “out of work” state and could result in the controller going into a “factory reset” state.	7.5	More Details
CVE-2022-28556	Tenda AC15 US_AC15V1.0BR_V15.03.05.20_multi_TDE01.bin is vulnerable to Buffer Overflow. The stack overflow vulnerability lies in the /goform/setpptpservercfg interface of the web. The sent post data startip and endip are copied to the stack using the sanf function, resulting in stack overflow. Similarly, this vulnerability can be used together with CVE-2021-44971	7.5	More Details
CVE-2022-23705	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays, HPE Nimble Storage All Flash Arrays, and HPE Nimble Storage Secondary Flash Arrays which could potentially allow the upload, but not execution, of unauthorized update binaries to the array. HPE has made the following software updates to resolve the vulnerability in HPE Nimble Storage: 5.0.10.100 or later, 5.2.1.0 or later, 6.0.0.100 or later.	7.5	More Details
CVE-2022-23704	A potential security vulnerability has been identified in Integrated Lights-Out 4 (iLO 4). The vulnerability could allow remote Denial of Service. The vulnerability is resolved in Integrated Lights-Out 4 (iLO 4) 2.80 and later.	7.5	More Details
CVE-2022-28488	The function wav_format_write in libwav.c in libwav through 2017-04-20 has an Use of Uninitialized Variable vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28691	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.5	More Details
CVE-2022-23443	An improper access control in Fortinet FortiSOAR before 7.2.0 allows unauthenticated attackers to access gateway API data via crafted HTTP GET requests.	7.5	More Details
CVE-2022-29117	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2022-22433	IBM Robotic Process Automation 21.0.1 and 21.0.2 is vulnerable to External Service Interaction attack, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to induce the application to perform server-side DNS lookups or HTTP requests to arbitrary domain names. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. IBM X-Force ID: 224156.	7.5	More Details
CVE-2022-26913	Windows Authentication Information Disclosure Vulnerability	7.4	More Details
CVE-2021-27764	Cookie without HTTPONLY flag set. NUMBER cookie(s) was set without Secure or HTTPOnly flags. The images show the cookie with the missing flag. (WebUI)	7.4	More Details
CVE-2022-26071	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a flaw in the way reply ICMP packets are limited in the Traffic Management Microkernel (TMM) allows an attacker to quickly scan open UDP ports. This flaw allows an off-path remote attacker to effectively bypass source port UDP randomization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29167	Hawk is an HTTP authentication scheme providing mechanisms for making authenticated HTTP requests with partial cryptographic verification of the request and response, covering the HTTP method, request URI, host, and optionally the request payload. Hawk used a regular expression to parse `Host` HTTP header (`Hawk.utils.parseHost()`), which was subject to regular expression DoS attack - meaning each added character in the attacker's input increases the computation time exponentially. `parseHost()` was patched in `9.0.1` to use built-in `URL` class to parse hostname instead. `Hawk.authenticate()` accepts `options` argument. If that contains `host` and `port`, those would be used instead of a call to `utils.parseHost()`.	7.4	More Details
CVE-2021-23792	The package com.twelvemonkeys.imageio:imageio-metadata before 3.7.1 are vulnerable to XML External Entity (XXE) Injection due to an insecurely initialized XML parser for reading XMP Metadata. An attacker can exploit this vulnerability if they are able to supply a file (e.g. when an online profile picture is processed) with a malicious XMP segment. If the XMP metadata of the uploaded image is parsed, then the XXE vulnerability is triggered.	7.3	More Details
CVE-2022-28714	On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, as well as F5 BIG-IP APM Clients 7.x versions prior to 7.2.1.5, a DLL Hijacking vulnerability exists in the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.3	More Details
CVE-2022-28695	On F5 BIG-IP AFM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, an authenticated attacker with high privileges can upload a maliciously crafted file to the BIG-IP AFM Configuration utility, which allows an attacker to run arbitrary commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.2	More Details
CVE-2022-27224	An issue was discovered in Galleon NTS-6002-GPS 4.14.103-Galleon-NTS-6002.V12 4. An authenticated attacker can perform command injection as root via shell metacharacters within the Network Tools section of the web-management interface. All three networking tools are affected (Ping, Traceroute, and DNS Lookup) and their respective input fields (ping_address, trace_address, nslookup_address).	7.2	More Details
CVE-2022-24899	Contao is a powerful open source CMS that allows you to create professional websites and scalable web applications. In versions of Contao prior to 4.13.3 it is possible to inject code into the canonical tag. As a workaround users may disable canonical tags in the root page settings.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28076	Seacms v11.6 was discovered to contain a remote command execution (RCE) vulnerability via the Mail Server Settings.	7.2	More Details
CVE-2022-28096	Skycaiji v2.4 was discovered to contain a remote code execution (RCE) vulnerability via /SkycaijiApp/admin/controller/Develop.php.	7.2	More Details
CVE-2021-26408	Insufficient validation of elliptic curve points in SEV-legacy firmware may compromise SEV-legacy guest migration potentially resulting in loss of guest's integrity or confidentiality.	7.1	More Details
CVE-2021-26370	Improper validation of destination address in SVC_LOAD_FW_IMAGE_BY_INSTANCE and SVC_LOAD_BINARY_BY_ATTRIB in a malicious UApp or ABL may allow an attacker to overwrite arbitrary bootloader memory with SPI ROM contents resulting in a loss of integrity and availability.	7.1	More Details
CVE-2022-27167	Privilege escalation vulnerability in Windows products of ESET, spol. s r.o. allows attacker to exploit "Repair" and "Uninstall" features what may lead to arbitrary file deletion. 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. ESET, spol. s r.o. ESET Endpoint Security 6.0 versions prior to 9.0.2046.0. 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.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44057	An improper authentication vulnerability has been reported to affect QNAP device running Photo Station. If exploited, this vulnerability allows attackers to compromise the security of the system. We have already fixed this vulnerability in the following versions of Photo Station: Photo Station 6.0.20 (2022/02/15) and later Photo Station 5.7.16 (2022/02/11) and later Photo Station 5.4.13 (2022/02/11) and later	7.1	More Details
CVE-2021-44056	An improper authentication vulnerability has been reported to affect QNAP device running Video Station. If exploited, this vulnerability allows attackers to compromise the security of the system. We have already fixed this vulnerability in the following versions of Video Station: Video Station 5.5.9 and later Video Station 5.3.13 and later Video Station 5.1.8 and later	7.1	More Details
CVE-2022-29164	Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. In affected versions an attacker can create a workflow which produces a HTML artifact containing an HTML file that contains a script which uses XHR calls to interact with the Argo Server API. The attacker emails the deep-link to the artifact to their victim. The victim opens the link, the script starts running. As the script has access to the Argo Server API (as the victim), so may read information about the victim's workflows, or create and delete workflows. Note the attacker must be an insider: they must have access to the same cluster as the victim and must already be able to run their own workflows. The attacker must have an understanding of the victim's system. We have seen no evidence of this in the wild. We urge all users to upgrade to the fixed versions.	7.1	More Details
CVE-2021-26332	Failure to verify SEV-ES TMR is not in MMIO space, SEV-ES FW could result in a potential loss of integrity or availability.	7.1	More Details
CVE-2022-29106	Windows Hyper-V Shared Virtual Disk Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-1537	file.copy operations in GruntJS are vulnerable to a TOCTOU race condition leading to arbitrary file write in GitHub repository gruntjs/grunt prior to 1.5.3. This vulnerability is capable of arbitrary file writes which can lead to local privilege escalation to the GruntJS user if a lower-privileged user has write access to both source and destination directories as the lower-privileged user can create a symlink to the GruntJS user's .bashrc file or replace /etc/shadow file if the GruntJS user is root.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20118	In ion_ioctl and related functions of ion.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-205707793References: N/A	7.0	More Details
CVE-2022-26939	Storage Spaces Direct Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-26938	Storage Spaces Direct Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-29138	Windows Clustered Shared Volume Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-23279	Windows ALPC Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-29135	Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-20006	In several functions of KeyguardServiceWrapper.java and related files,, there is a possible way to briefly view what's under the lockscreen due to a race condition. This could lead to local escalation of privilege if a Guest user is enabled, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-151095871	7.0	More Details
CVE-2022-22016	Windows PlayToManager Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-20007	In startActivityForAttachedApplicationIfNeeded of RootWindowContainer.java, there is a possible way to overlay an app that believes it's still in the foreground, when it is not, due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-211481342	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29125	Windows Push Notifications Apps Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-29142	Windows Kernel Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-29150	Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-38445	OCI OpenDDS versions prior to 3.18.1 do not handle a length parameter consistent with the actual length of the associated data, which may allow an attacker to remotely execute arbitrary code.	7.0	More Details
CVE-2022-29126	Tablet Windows User Interface Application Core Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-29151	Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-27878	On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	6.8	More Details
CVE-2022-20009	In various functions of the USB gadget subsystem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-213172319References: Upstream kernel	6.8	More Details
CVE-2021-25267	Multiple XSS vulnerabilities in Webadmin allow for privilege escalation from admin to super-admin in Sophos Firewall older than version 19.0 GA.	6.8	More Details
CVE-2021-27765	The BigFix Server API installer is created with InstallShield, which was affected by CVE-2021-41526, a vulnerability that could allow a local user to perform a privilege escalation. This vulnerability was resolved by updating to an InstallShield version with the underlying vulnerability fixed.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27767	The BigFix Console installer is created with InstallShield, which was affected by CVE-2021-41526, a vulnerability that could allow a local user to perform a privilege escalation. This vulnerability was resolved by updating to an InstallShield version with the underlying vulnerability fixed.	6.7	More Details
CVE-2021-27766	The BigFix Client installer is created with InstallShield, which was affected by CVE-2021-41526, a vulnerability that could allow a local user to perform a privilege escalation. This vulnerability was resolved by updating to an InstallShield version with the underlying vulnerability fixed.	6.7	More Details
CVE-2021-38435	RTI Connext DDS Professional and Connext DDS Secure Versions 4.2x to 6.1.0 not correctly calculate the size when allocating the buffer, which may result in a buffer overflow.	6.6	More Details
CVE-2021-38433	RTI Connext DDS Professional and Connext DDS Secure Versions 4.2x to 6.1.0 vulnerable to a stack-based buffer overflow, which may allow a local attacker to execute arbitrary code.	6.6	More Details
CVE-2021-38441	Eclipse CycloneDDS versions prior to 0.8.0 are vulnerable to a write-what-where condition, which may allow an attacker to write arbitrary values in the XML parser.	6.6	More Details
CVE-2021-38443	Eclipse CycloneDDS versions prior to 0.8.0 improperly handle invalid structures, which may allow an attacker to write arbitrary values in the XML parser.	6.6	More Details
CVE-2021-38429	OCI OpenDDS versions prior to 3.18.1 are vulnerable when an attacker sends a specially crafted packet to flood target devices with unwanted traffic, which may result in a denial-of-service condition and information exposure.	6.6	More Details
CVE-2021-38427	RTI Connext DDS Professional and Connext DDS Secure Versions 4.2.x to 6.1.0 are vulnerable to a stack-based buffer overflow, which may allow a local attacker to execute arbitrary code.	6.6	More Details
CVE-2021-38423	All versions of GurumDDS improperly calculate the size to be used when allocating the buffer, which may result in a buffer overflow.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29171	Sourcegraph is a fast and featureful code search and navigation engine. Versions before 3.38.0 are vulnerable to Remote Code Execution in the gitserver service. The Gitolite code host integration with Phabricator allows Sourcegraph site admins to specify a `callsignCommand`, which is used to obtain the Phabricator metadata for a Gitolite repository. An administrator who is able to edit or add a Gitolite code host and has administrative access to Sourcegraph's bundled Grafana instance can change this command arbitrarily and run it remotely. This grants direct access to the infrastructure underlying the Sourcegraph installation. The attack requires: site-admin privileges on the instance of Sourcegraph, Administrative privileges on the bundled Grafana monitoring instance, Knowledge of the gitserver IP address or DNS name (if running in Kubernetes). This can be found through Grafana. The issue is patched in version 3.38.0. You may disable Gitolite code hosts. We still highly encourage upgrading regardless of workarounds.	6.6	More Details
CVE-2022-1476	The All-in-One WP Migration plugin for WordPress is vulnerable to arbitrary file deletion via directory traversal due to insufficient file validation via the ~/lib/model/class-ai1wm-backups.php file, in versions up to, and including, 7.58. This can be exploited by administrative users, and users who have access to the site's secret key.	6.6	More Details
CVE-2022-30330	In the KeepKey firmware before 7.3.2,Flaws in the supervisor interface can be exploited to bypass important security restrictions on firmware operations. Using these flaws, malicious firmware code can elevate privileges, permanently make the device inoperable or overwrite the trusted bootloader code to compromise the hardware wallet across reboots or storage wipes.	6.6	More Details
CVE-2022-25785	Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7.	6.6	More Details
CVE-2022-26936	Windows Server Service Information Disclosure Vulnerability	6.5	More Details
CVE-2022-26073	A denial of service vulnerability exists in the libxm_av.so DemuxCmdInBuffer functionality of Anker Eufy Homebase 2 2.1.8.5h. A specially-crafted set of network packets can lead to a device reboot. An attacker can send packets to trigger this vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20796	On May 4, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in Clam AntiVirus (ClamAV) versions 0.103.4, 0.103.5, 0.104.1, and 0.104.2 could allow an authenticated, local attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog.	6.5	More Details
CVE-2022-20794	Multiple vulnerabilities in the web engine of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow a remote attacker to cause a denial of service (DoS) condition, view sensitive data on an affected device, or redirect users to an attacker-controlled destination. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2022-20764	Multiple vulnerabilities in the web engine of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow a remote attacker to cause a denial of service (DoS) condition, view sensitive data on an affected device, or redirect users to an attacker-controlled destination. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2022-20010	In l2cble_process_sig_cmd of l2c_ble.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure through Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-213519176	6.5	More Details
CVE-2022-29112	Windows Graphics Component Information Disclosure Vulnerability	6.5	More Details
CVE-2022-29120	Windows Clustered Shared Volume Information Disclosure Vulnerability	6.5	More Details
CVE-2022-29121	Windows WLAN AutoConfig Service Denial of Service Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44052	An improper link resolution before file access ('Link Following') vulnerability has been reported to affect QNAP device running QuTScloud, QuTS hero, and QTS. If exploited, this vulnerability allows remote attackers to traverse the file system to unintended locations and read or overwrite the contents of unexpected files. We have already fixed this vulnerability in the following versions of QuTScloud, QuTS hero, and QTS: QuTScloud c5.0.1.1998 and later QuTS hero h4.5.4.1971 build 20220310 and later QuTS hero h5.0.0.1986 build 20220324 and later QTS 4.3.4.1976 build 20220303 and later QTS 4.3.3.1945 build 20220303 and later QTS 4.2.6 build 20220304 and later QTS 4.3.6.1965 build 20220302 and later QTS 5.0.0.1986 build 20220324 and later QTS 4.5.4.1991 build 20220329 and later	6.5	More Details
CVE-2022-29122	Windows Clustered Shared Volume Information Disclosure Vulnerability	6.5	More Details
CVE-2022-29123	Windows Clustered Shared Volume Information Disclosure Vulnerability	6.5	More Details
CVE-2022-27495	On all versions 1.3.x (fixed in 1.4.0) NGINX Service Mesh control plane endpoints are exposed to the cluster overlay network. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	6.5	More Details
CVE-2022-27634	On 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, BIG-IP APM does not properly validate configurations, allowing an authenticated attacker with high privileges to manipulate the APM policy leading to privilege escalation/remote code execution. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	6.5	More Details
CVE-2022-28859	On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24041	A vulnerability has been identified in Desigo DXR2 (All versions < V01.21.142.5-22), Desigo PXC3 (All versions < V01.21.142.4-18), Desigo PXC4 (All versions < V02.20.142.10-10884), Desigo PXC5 (All versions < V02.20.142.10-10884). The web application stores the PBKDF2 derived key of users passwords with a low iteration count. An attacker with user profile access privilege can retrieve the stored password hashes of other accounts and then successfully perform an offline cracking attack and recover the plaintext passwords of other users.	6.5	More Details
CVE-2022-27337	A logic error in the Hints::Hints function of Poppler v22.03.0 allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.	6.5	More Details
CVE-2022-24040	A vulnerability has been identified in Desigo DXR2 (All versions < V01.21.142.5-22), Desigo PXC3 (All versions < V01.21.142.4-18), Desigo PXC4 (All versions < V02.20.142.10-10884), Desigo PXC5 (All versions < V02.20.142.10-10884). The web application fails to enforce an upper bound to the cost factor of the PBKDF2 derived key during the creation or update of an account. An attacker with the user profile access privilege could cause a denial of service (DoS) condition through CPU consumption by setting a PBKDF2 derived key with a remarkably high cost effort and then attempting a login to the so-modified account.	6.5	More Details
CVE-2022-26934	Windows Graphics Component Information Disclosure Vulnerability	6.5	More Details
CVE-2022-28090	Jspxcms v10.2.0 allows attackers to execute a Server-Side Request Forgery (SSRF) via /cmscp/ext/collect/fetch_url.do?url=.	6.5	More Details
CVE-2022-28471	In ffjpeg (commit hash: caade60), the function bmp_load() in bmp.c contains an integer overflow vulnerability, which eventually results in the heap overflow in jfif_encode() in jfif.c. This is due to the incomplete patch for issue 38	6.5	More Details
CVE-2022-29943	Talend Administration Center has a vulnerability that allows an authenticated user to use XML External Entity (XXE) processing to achieve read access as root on the remote filesystem. The issue is fixed for versions 8.0.x in TPS-5189, versions 7.3.x in TPS-5175, and versions 7.2.x in TPS-5201. Earlier versions of Talend Administration Center may also be impacted; users are encouraged to update to a supported version.	6.5	More Details
CVE-2022-22015	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30295	uClibc-ng through 1.0.40 and uClibc through 0.9.33.2 use predictable DNS transaction IDs that may lead to DNS cache poisoning. This is related to a reset of a value to 0x2.	6.5	More Details
CVE-2022-26940	Remote Desktop Protocol Client Information Disclosure Vulnerability	6.5	More Details
CVE-2022-29942	Talend Administration Center has a vulnerability that allows an authenticated user to use the Service Registry 'Add' functionality to perform SSRF HTTP GET requests on URLs in the internal network. The issue is fixed for versions 8.0.x in TPS-5189, versions 7.3.x in TPS-5175, and versions 7.2.x in TPS-5201. Earlier versions of Talend Administration Center may also be impacted; users are encouraged to update to a supported version.	6.5	More Details
CVE-2022-28164	Brocade SANnav before SANnav 2.2.0 application uses the Blowfish symmetric encryption algorithm for the storage of passwords. This could allow an authenticated attacker to decrypt stored account passwords.	6.5	More Details
CVE-2022-26935	Windows WLAN AutoConfig Service Information Disclosure Vulnerability	6.5	More Details
CVE-2022-29134	Windows Clustered Shared Volume Information Disclosure Vulnerability	6.5	More Details
CVE-2022-22415	A vulnerability exists where an IBM Robotic Process Automation 21.0.1 regular user is able to obtain view-only access to some admin pages in the Control Center IBM X-Force ID: 223029.	6.5	More Details
CVE-2022-28601	A Two-Factor Authentication (2FA) bypass vulnerability in "Simple 2FA Plugin for Moodle" by LMS Doctor allows remote attackers to overwrite the phone number used for confirmation via the profile.php file. Therefore, allowing them to bypass the phone verification mechanism.	6.5	More Details
CVE-2022-23724	Use of static encryption key material allows forging an authentication token to other users within a tenant organization. MFA may be bypassed by redirecting an authentication flow to a target user. To exploit the vulnerability, must have compromised user credentials.	6.4	More Details
CVE-2021-41032	An improper access control vulnerability [CWE-284] in FortiOS versions 6.4.8 and prior and 7.0.3 and prior may allow an authenticated attacker with a restricted user profile to gather sensitive information and modify the SSL-VPN tunnel status of other VDOMs using specific CLI commands.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26390	A malicious or compromised UApp or ABL may coerce the bootloader into corrupting arbitrary memory potentially leading to loss of integrity of data.	6.2	More Details
CVE-2022-1567	The WP-JS plugin for WordPress contains a script called wp-js.php with the function wp_js_admin, that accepts unvalidated user input and echoes it back to the user. This can be used for reflected Cross-Site Scripting in versions up to, and including, 2.0.6.	6.1	More Details
CVE-2021-39024	IBM Guardium Data Encryption (GDE) 4.0.0.0 and 5.0.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 213862.	6.1	More Details
CVE-2022-1571	Cross-site scripting - Reflected in Create Subaccount in GitHub repository neorazorx/facturascripts prior to 2022.07. This vulnerability can be arbitrarily executed javascript code to steal user'cookie, perform HTTP request, get content of `same origin` page, etc ...	6.1	More Details
CVE-2022-30241	The jquery.json-viewer library through 1.4.0 for Node.js does not properly escape characters such as < in a JSON object, as demonstrated by a SCRIPT element.	6.1	More Details
CVE-2022-29172	Auth0 is an authentication broker that supports both social and enterprise identity providers, including Active Directory, LDAP, Google Apps, and Salesforce. In versions before `11.33.0`, when the “additional signup fields” feature [is configured](https://github.com/auth0/lock#additional-sign-up-fields), a malicious actor can inject invalidated HTML code into these additional fields, which is then stored in the service `user_metdata` payload (using the `name` property). Verification emails, when applicable, are generated using this metadata. It is therefor possible for an actor to craft a malicious link by injecting HTML, which is then rendered as the recipient's name within the delivered email template. You are impacted by this vulnerability if you are using `auth0-lock` version `11.32.2` or lower and are using the “additional signup fields” feature in your application. Upgrade to version `11.33.0`.	6.1	More Details
CVE-2022-1411	Unrestructed file upload in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0. Attacker can send malicious files to the victims is able to retrieve the stored data from the web application without that data being made safe to render in the browser and steals victim's cookie leads to account takeover.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1584	Reflected XSS in GitHub repository microweber/microweber prior to 1.2.16. Executing JavaScript as the victim	6.1	More Details
CVE-2022-1047	The Themify Post Type Builder Search Addon WordPress plugin before 1.4.0 does not properly escape the current page URL before reusing it in a HTML attribute, leading to a reflected cross site scripting vulnerability.	6.1	More Details
CVE-2022-0625	The Admin Menu Editor WordPress plugin through 1.0.4 does not sanitize and escape a parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-1555	DOM XSS in microweber ver 1.2.15 in GitHub repository microweber/microweber prior to 1.2.16. inject arbitrary js code, deface website, steal cookie...	6.1	More Details
CVE-2022-27461	In nopCommerce 4.50.1, an open redirect vulnerability can be triggered by luring a user to authenticate to a nopCommerce page by clicking on a crafted link.	6.1	More Details
CVE-2022-28081	A reflected cross-site scripting (XSS) vulnerability in the component Query.php of arPHP v3.6.0 allows attackers to execute arbitrary web scripts.	6.1	More Details
CVE-2022-30278	A vulnerability in Black Duck Hub’s embedded MadCap Flare documentation files could allow an unauthenticated remote attacker to conduct a cross-site scripting attack. The vulnerability is due to improper validation of user-supplied input to MadCap Flare's framework embedded within Black Duck Hub's Help Documentation to supply content. An attacker could exploit this vulnerability by convincing a user to click a link designed to pass malicious input to the interface. A successful exploit could allow the attacker to conduct cross-site scripting attacks and gain access to sensitive browser-based information.	6.1	More Details
CVE-2022-28508	An XSS issue was discovered in browser_search_plugin.php in MantisBT before 2.25.2. Unescaped output of the return parameter allows an attacker to inject code into a hidden input field.	6.1	More Details
CVE-2022-1171	The Vertical scroll recent post WordPress plugin before 14.0 does not sanitise and escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26370	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.9	More Details
CVE-2022-29420	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Adam Skaat Countdown & Clock (WordPress plugin) countdown-builder allows Stored XSS.This issue affects Countdown & Clock (WordPress plugin): from n/a through 2.3.2.	5.9	More Details
CVE-2022-26517	On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.9	More Details
CVE-2022-28706	On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.9	More Details
CVE-2022-28708	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.9	More Details
CVE-2022-29473	On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29180	A vulnerability in which attackers could forge HTTP requests to manipulate the `charm` data directory to access or delete anything on the server. This has been patched and is available in release [v0.12.1](https://github.com/charmbracelet/charm/releases/tag/v0.12.1). We recommend that all users running self-hosted `charm` instances update immediately. This vulnerability was found in-house and we haven't been notified of any potential exploiters. ### Additional notes * Encrypted user data uploaded to the Charm server is safe as Charm servers cannot decrypt user data. This includes filenames, paths, and all key-value data. * Users running the official Charm [Docker images](https://github.com/charmbracelet/charm/blob/main/docker.md) are at minimal risk because the exploit is limited to the containerized filesystem.	5.9	More Details
CVE-2021-44053	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running QTS, QuTS hero and QuTScloud. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of QTS, QuTS hero and QuTScloud: QTS 4.5.4.1991 build 20220329 and later QTS 5.0.0.1986 build 20220324 and later QuTS hero h5.0.0.1986 build 20220324 and later QuTS hero h4.5.4.1971 build 20220310 and later QuTScloud c5.0.1.1949 and later	5.7	More Details
CVE-2021-32010	Inadequate Encryption Strength vulnerability in TLS stack of Secomea SiteManager, LinkManager, GateManager may facilitate man in the middle attacks. This issue affects: Secomea SiteManager All versions prior to 9.7. Secomea LinkManager versions prior to 9.7. Secomea GateManager versions prior to 9.7.	5.6	More Details
CVE-2022-22713	Windows Hyper-V Denial of Service Vulnerability	5.6	More Details
CVE-2022-20121	In getNodeValue of USCCDMPlugin.java, there is a possible disclosure of ICCID due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-212573046References: N/A	5.5	More Details
CVE-2022-27114	There is a vulnerability in htmldoc 1.9.16. In image_load_jpeg function image.cxx when it calls malloc,'img->width' and 'img->height' they are large enough to cause an integer overflow. So, the malloc function may return a heap blosmaller than the expected size, and it will cause a buffer overflow/Address boundary error in the jpeg_read_scanlines function.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20011	In getArray of NotificationManagerService.java , there is a possible leak of one user notifications to another due to missing check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-214999128	5.5	More Details
CVE-2022-20112	In getAvailabilityStatus of PrivateDnsPreferenceController.java, there is a possible way for a guest user to change private DNS settings due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-206987762	5.5	More Details
CVE-2022-20115	In broadcastServiceStateChanged of TelephonyRegistry.java, there is a possible way to learn base station information without location permission due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-210118427	5.5	More Details
CVE-2022-27359	Foxit PDF Reader before 12.0.1 and PDF Editor before 12.0.1 allow a this.maildoc NULL pointer dereference.	5.5	More Details
CVE-2022-20119	In private_handle_t of mali_gralloc_buffer.h, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-213170715References: N/A	5.5	More Details
CVE-2022-24823	Netty is an open-source, asynchronous event-driven network application framework. The package `io.netty:netty-codec-http` prior to version 4.1.77.Final contains an insufficient fix for CVE-2021-21290. When Netty's multipart decoders are used local information disclosure can occur via the local system temporary directory if temporary storing uploads on the disk is enabled. This only impacts applications running on Java version 6 and lower. Additionally, this vulnerability impacts code running on Unix-like systems, and very old versions of Mac OSX and Windows as they all share the system temporary directory between all users. Version 4.1.77.Final contains a patch for this vulnerability. As a workaround, specify one's own `java.io.tmpdir` when starting the JVM or use DefaultHttpDataFactory.setBaseDir(...) to set the directory to something that is only readable by the current user.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22011	Windows Graphics Component Information Disclosure Vulnerability	5.5	More Details
CVE-2021-39670	In setStream of WallpaperManager.java, there is a possible way to cause a permanent DoS due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-204087139	5.5	More Details
CVE-2022-1516	A NULL pointer dereference flaw was found in the Linux kernel's X.25 set of standardized network protocols functionality in the way a user terminates their session using a simulated Ethernet card and continued usage of this connection. This flaw allows a local user to crash the system.	5.5	More Details
CVE-2022-26930	Windows Remote Access Connection Manager Information Disclosure Vulnerability	5.5	More Details
CVE-2022-26933	Windows NTFS Information Disclosure Vulnerability	5.5	More Details
CVE-2022-29102	Windows Failover Cluster Information Disclosure Vulnerability	5.5	More Details
CVE-2022-29140	Windows Print Spooler Information Disclosure Vulnerability	5.5	More Details
CVE-2022-29107	Microsoft Office Security Feature Bypass Vulnerability	5.5	More Details
CVE-2022-29114	Windows Print Spooler Information Disclosure Vulnerability	5.5	More Details
CVE-2021-39700	In the policies of adbd.te, there was a logic error which caused the CTS Listening Ports Test to report invalid results. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-201645790	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20117	In (TBD) of (TBD), there is a possible way to decrypt local data encrypted by the GSC due to improperly used crypto. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-217475903References: N/A	5.5	More Details
CVE-2022-28161	An information exposure through log file vulnerability in Brocade SANNav versions before Brocade SANnav 2.2.0 could allow an authenticated, local attacker to view sensitive information such as ssh passwords in filetansfer.log in debug mode. To exploit this vulnerability, the attacker would need to have valid user credentials and turn on debug mode.	5.5	More Details
CVE-2021-26352	Insufficient bound checks in System Management Unit (SMU) PCIe Hot Plug table may result in access/updates from/to invalid address space that could result in denial of service.	5.5	More Details
CVE-2022-29868	1Password for Mac 7.2.4 through 7.9.x before 7.9.3 is vulnerable to a process validation bypass. Malicious software running on the same computer can exfiltrate secrets from 1Password provided that 1Password is running and is unlocked. Affected secrets include vault items and derived values used for signing in to 1Password.	5.5	More Details
CVE-2022-27875	On F5 Access for Android 3.x versions prior to 3.0.8, a Task Hijacking vulnerability exists in the F5 Access for Android application, which may allow an attacker to steal sensitive user information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.5	More Details
CVE-2022-1649	Null pointer dereference in libr/bin/format/mach0/mach0.c in radareorg/radare2 in GitHub repository radareorg/radare2 prior to 5.7.0. It is likely to be exploitable. For more general description of heap buffer overflow, see [CWE](https://cwe.mitre.org/data/definitions/476.html).	5.5	More Details
CVE-2022-27636	On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, as well as F5 BIG-IP APM Clients 7.x versions prior to 7.2.1.5, BIG-IP Edge Client may log sensitive APM session-related information when VPN is launched on a Windows system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.5	More Details
CVE-2022-29940	In LibreHealth EHR 2.0.0, lack of sanitization of the GET parameters formseq and formid in interface\orders\find_order_popup.php leads to multiple cross-site scripting (XSS) vulnerabilities.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27308	A stored cross-site scripting (XSS) vulnerability in PHProjekt PhpSimplyGest v1.3.0 allows attackers to execute arbitrary web scripts or HTML via a project title.	5.4	More Details
CVE-2022-1464	Stored xss bug in GitHub repository gogs/gogs prior to 0.12.7. As the repo is public , any user can view the report and when open the attachment then xss is executed. This bug allow executed any javascript code in victim account .	5.4	More Details
CVE-2022-0898	The IgniteUp WordPress plugin through 3.4.1 does not sanitise and escape some fields when high privilege users don't have the unfiltered_html capability, which could lead to Stored Cross-Site Scripting issues	5.4	More Details
CVE-2022-29161	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The XWiki Crypto API will generate X509 certificates signed by default using SHA1 with RSA, which is not considered safe anymore for use in certificate signatures, due to the risk of collisions with SHA1. The problem has been patched in XWiki version 13.10.6, 14.3.1 and 14.4-rc-1. Since then, the Crypto API will generate X509 certificates signed by default using SHA256 with RSA. Administrators are advised to upgrade their XWiki installation to one of the patched versions. If the upgrade is not possible, it is possible to patch the module xwiki-platform-crypto in a local installation by applying the change exposed in 26728f3 and re-compiling the module.	5.4	More Details
CVE-2021-43712	Stored XSS in Add New Employee Form in Sourcecodester Employee Daily Task Management System 1.0 Allows Remote Attacker to Inject/Store Arbitrary Code via the Name Field.	5.4	More Details
CVE-2022-29939	In LibreHealth EHR 2.0.0, lack of sanitization of the GET parameters debug and InsId in interface\billing\sl_eob_process.php leads to multiple cross-site scripting (XSS) vulnerabilities.	5.4	More Details
CVE-2022-25782	Improper Handling of Insufficient Privileges vulnerability in Web UI of Secomea GateManager allows logged in user to access and update privileged information. This issue affects: Secomea GateManager versions prior to 9.7.	5.4	More Details
CVE-2022-22319	IBM Robotic Process Automation 21.0.1 could allow a register user on the system to physically delete a queue that could cause disruption for any scripts dependent on the queue. IBM X-Force ID: 218366.	5.4	More Details
CVE-2021-36912	Stored Cross-Site Scripting (XSS) vulnerability in Andrea Pernici News Sitemap for Google plugin <= 1.0.16 on WordPress, attackers must have contributor or higher user role.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28545	FUDforum 3.1.1 is vulnerable to Stored XSS.	5.4	More Details
CVE-2022-29479	On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.3	More Details
CVE-2022-29480	On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.3	More Details
CVE-2021-39020	IBM Guardium Data Encryption (GDE) 4.0.0.7 and lower stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 213855.	5.3	More Details
CVE-2022-27182	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.3	More Details
CVE-2021-33845	The Splunk Enterprise REST API allows enumeration of usernames via the lockout error message. The potential vulnerability impacts Splunk Enterprise instances before 8.1.7 when configured to repress verbose login errors.	5.3	More Details
CVE-2022-27181	On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when APM is configured on a virtual server and the associated access profile is configured with APM AAA NTLM Auth, undisclosed requests can cause an increase in internal resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30334	Brave before 1.34, when a Private Window with Tor Connectivity is used, leaks .onion URLs in Referer and Origin headers. NOTE: although this was fixed by Brave, the Brave documentation still advises "Note that Private Windows with Tor Connectivity in Brave are just regular private windows that use Tor as a proxy. Brave does NOT implement most of the privacy protections from Tor Browser."	5.3	More Details
CVE-2021-44055	An missing authorization vulnerability has been reported to affect QNAP device running Video Station. If exploited, this vulnerability allows remote attackers to access data or perform actions that they should not be allowed to perform. We have already fixed this vulnerability in the following versions of Video Station: Video Station 5.5.9 (2022/02/16) and later	5.3	More Details
CVE-2022-0424	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users	5.3	More Details
CVE-2022-25990	On 1.0.x versions prior to 1.0.1, systems running F5OS-A software may expose certain registry ports externally. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.3	More Details
CVE-2021-38693	A path traversal vulnerability has been reported to affect QNAP device running QuTScloud, QuTS hero, QTS, QVR Pro Appliance. If exploited, this vulnerability allows attackers to read the contents of unexpected files and expose sensitive data. We have already fixed this vulnerability in the following versions of QuTScloud, QuTS hero, QTS, QVR Pro Appliance: QuTScloud c5.0.1.1949 and later QuTS hero h5.0.0.1949 build 20220215 and later QuTS hero h4.5.4.1951 build 20220218 and later QTS 5.0.0.1986 build 20220324 and later QTS 4.5.4.1991 build 20220329 and later	5.3	More Details
CVE-2022-26130	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an Active mode-enabled FTP profile is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing active FTP data channel connections. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22481	IBM Navigator for i 7.2, 7.3, and 7.4 (heritage version) could allow a remote attacker to obtain access to the web interface without valid credentials. By modifying the sign on request, an attacker can gain visibility to the fully qualified domain name of the target system and the navigator tasks page, however they do not gain the ability to perform those tasks on the system or see any specific system data. IBM X-Force ID: 225899.	5.3	More Details
CVE-2022-0866	This is a concurrency issue that can result in the wrong caller principal being returned from the session context of an EJB that is configured with a RunAs principal. In particular, the org.jboss.as.ejb3.component.EJBComponent class has an incomingRunAsIdentity field. This field is used by the org.jboss.as.ejb3.security.RunAsPrincipalInterceptor to keep track of the current identity prior to switching to a new identity created using the RunAs principal. The exploit consist that the EJBComponent#incomingRunAsIdentity field is currently just a SecurityIdentity. This means in a concurrent environment, where multiple users are repeatedly invoking an EJB that is configured with a RunAs principal, it's possible for the wrong the caller principal to be returned from EJBComponent#getCallerPrincipal. Similarly, it's also possible for EJBComponent#isCallerInRole to return the wrong value. Both of these methods rely on incomingRunAsIdentity. Affects all versions of JBoss EAP from 7.1.0 and all versions of WildFly 11+ when Elytron is enabled.	5.3	More Details
CVE-2019-25060	The WPGraphQL WordPress plugin before 0.3.5 doesn't properly restrict access to information about other users' roles on the affected site. Because of this, a remote attacker could forge a GraphQL query to retrieve the account roles of every user on the site.	5.3	More Details
CVE-2021-39027	IBM Guardium Data Encryption (GDE) 4.0.0 and 5.0.0 prepares a structured message for communication with another component, but encoding or escaping of the data is either missing or done incorrectly. As a result, the intended structure of the message is not preserved. IBM X-Force ID: 213865.	5.0	More Details
CVE-2022-26340	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19212	SQL Injection vulnerability in admin/group_list.php in piwigo v2.9.5, via the group parameter to delete.	4.9	More Details
CVE-2022-25786	Unprotected Alternate Channel vulnerability in debug console of GateManager allows system administrator to obtain sensitive information. This issue affects: GateManager all versions prior to 9.7.	4.9	More Details
CVE-2022-26835	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal vulnerabilities exist in undisclosed iControl REST endpoints and TMOS Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	4.9	More Details
CVE-2022-0874	The WP Social Buttons WordPress plugin through 2.1 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-28507	Dragon Path Technologies Bharti Airtel Routers Hardware BDT-121 version 1.0 is vulnerable to Cross Site Scripting (XSS) via Dragon path router admin page.	4.8	More Details
CVE-2022-1104	The Popup Maker WordPress plugin before 1.16.5 does not sanitise and escape some of its Popup settings, 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-2022-27662	On F5 Traffix SDC 5.2.x versions prior to 5.2.2 and 5.1.x versions prior to 5.1.35, a stored Cross-Site Template Injection vulnerability exists in an undisclosed page of the Traffix SDC Configuration utility that allows an attacker to execute template language-specific instructions in the context of the server. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	4.8	More Details
CVE-2022-1303	The Slide Anything WordPress plugin before 2.3.44 does not sanitize and escape sliders' description, which could allow high privilege users such as editor and above to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27880	On F5 Traffix SDC 5.2.x versions prior to 5.2.2 and 5.1.x versions prior to 5.1.35, a stored Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the Traffix SDC Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	4.8	More Details
CVE-2022-29422	Multiple Authenticated (admin+) Persistent Cross-Site Scripting (XSS) vulnerabilities in Adam Skaat's Countdown & Clock plugin <= 2.3.2 at WordPress via &ycd-countdown-width, &ycd-progress-height, &ycd-progress-width, &ycd-button-margin-top, &ycd-button-margin-right, &ycd-button-margin-bottom, &ycd-button-margin-left, &ycd-circle-countdown-before-countdown, &ycd-circle-countdown-after-countdown vulnerable parameters.	4.8	More Details
CVE-2021-27761	Weak web transport security (Weak TLS): An attacker may be able to decrypt the data using attacks	4.8	More Details
CVE-2022-1338	The Easily Generate Rest API Url WordPress plugin through 1.0.0 does not escape some of its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-20753	A vulnerability in web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to an affected device. A successful exploit could allow the attacker to execute remote code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	4.7	More Details
CVE-2021-27762	Misconfigured security-related HTTP headers: Several security-related headers were missing or mis-configured on the web responses	4.7	More Details
CVE-2022-29116	Windows Kernel Information Disclosure Vulnerability	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20799	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.	4.7	More Details
CVE-2022-29421	Reflected Cross-Site Scripting (XSS) vulnerability in Adam Skaat's Countdown & Clock plugin on WordPress via &ycd_type vulnerable parameter.	4.7	More Details
CVE-2022-20801	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.	4.7	More Details
CVE-2021-45783	Bookeen Notea Firmware BK_R_1.0.5_20210608 is affected by a directory traversal vulnerability that allows an attacker to obtain sensitive information.	4.6	More Details
CVE-2022-20008	In mmc_blk_read_single of block.c, there is a possible way to read kernel heap memory due to uninitialized data. This could lead to local information disclosure if reading from an SD card that triggers errors, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-216481035References: Upstream kernel	4.6	More Details
CVE-2021-27760	An issue was discovered in the Sametime chat feature in the Notes 11.0 - 11.0.1 FP4 clients. An authenticated Sametime chat user could cause Remote Code Execution on another chat client by sending a specially formatted message through chat containing Javascript code.	4.6	More Details
CVE-2022-22434	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a user with physical access to create an API request modified to create additional objects. IBM X-Force ID: 224159.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20734	A vulnerability in Cisco SD-WAN vManage Software could allow an authenticated, local attacker to view sensitive information on an affected system. This vulnerability is due to insufficient file system restrictions. An authenticated attacker with netadmin privileges could exploit this vulnerability by accessing the vshell of an affected system. A successful exploit could allow the attacker to read sensitive information on the underlying operating system.	4.4	More Details
CVE-2021-27751	HCL Commerce is affected by an Insufficient Session Expiration vulnerability. After the session expires, in some circumstances, parts of the application are still accessible.	4.4	More Details
CVE-2021-44054	An open redirect vulnerability has been reported to affect QNAP device running QuTScloud, QuTS hero and QTS. If exploited, this vulnerability allows attackers to redirect users to an untrusted page that contains malware. We have already fixed this vulnerability in the following versions of QuTScloud, QuTS hero and QTS: QuTScloud c5.0.1.1949 and later QuTS hero h5.0.0.1949 build 20220215 and later QuTS hero h4.5.4.1951 build 20220218 and later QTS 5.0.0.1986 build 20220324 and later QTS 4.5.4.1991 build 20220329 and later	4.3	More Details
CVE-2021-43206	A server-generated error message containing sensitive information in Fortinet FortiOS 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.x, 6.0.x and FortiProxy 7.0.0 through 7.0.1, 2.0.x allows malicious webservers to retrieve a web proxy's client username and IP via same origin HTTP requests triggering proxy-generated HTTP status codes pages.	4.3	More Details
CVE-2022-1209	The Ultimate Member plugin for WordPress is vulnerable to arbitrary redirects due to insufficient validation on supplied URLs in the social fields of the Profile Page, which makes it possible for attackers to redirect unsuspecting victims in versions up to, and including, 2.3.1.	4.3	More Details
CVE-2021-27758	There is a security vulnerability in login form related to Cross-site Request Forgery which prevents user to login after attacker spam to login and system blocked victim's account.	4.3	More Details
CVE-2022-26070	When handling a mismatched pre-authentication cookie, the application leaks the internal error message in the response, which contains the Splunk Enterprise local system path. The vulnerability impacts Splunk Enterprise versions before 8.1.0.	4.3	More Details
CVE-2022-1468	On all versions of 17.0.x, 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x on F5 BIG-IP, an authenticated iControl REST user with at least guest role privileges can cause processing delays to iControl REST requests via undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1431	An issue has been discovered in GitLab affecting all versions starting from 12.10 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 requests to the PyPi API endpoint allowing the attacker to cause uncontrolled resource consumption.	4.3	More Details
CVE-2022-27659	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created by other BIG-IP users in the Traffic Management User Interface (TMUI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	4.3	More Details
CVE-2022-27909	In Joomla component 'jDownloads 3.9.8.2 Stable' the remote user can change some parameters in the address bar and see the names of other users' files	4.3	More Details
CVE-2022-25783	Insufficient Logging vulnerability in web server of Secomea GateManager allows logged in user to issue improper queries without logging. This issue affects: Secomea GateManager versions prior to 9.7.	4.3	More Details
CVE-2022-25780	Information Exposure vulnerability in web UI of Secomea GateManager allows logged in user to query devices outside own scope.	4.3	More Details
CVE-2022-29474	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	4.3	More Details
CVE-2022-25779	Logging of Excessive Data vulnerability in audit log of Secomea GateManager allows logged in user to write text entries in audit log. This issue affects: Secomea GateManager versions prior to 9.7.	4.3	More Details
CVE-2022-29950	Experian Hunter 1.16 allows remote authenticated users to modify assumed-immutable elements via the (1) rule name parameter to the Rules page or the (2) subrule name or (3) categories name parameter to the Subrules page. NOTE: the vendor disputes this because version 1.16 has never existed	4.3	More Details
CVE-2022-1502	Permissions were not properly verified in the API on projects using version control in Git. This allowed projects to be modified by users with only ProjectView permissions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1417	Improper access control in GitLab CE/EE affecting all versions starting from 8.12 before 14.8.6, all versions starting from 14.9 before 14.9.4, and all versions starting from 14.10 before 14.10.1 allows non-project members to access contents of Project Members-only Wikis via malicious CI jobs	4.3	More Details
CVE-2022-25781	Cross-site Scripting (XSS) vulnerability in Web UI of Secomea GateManager allows phishing attacker to inject javascript or html into logged in user session.	4.2	More Details
CVE-2022-29127	BitLocker Security Feature Bypass Vulnerability	4.2	More Details
CVE-2022-25778	Cross-Site Request Forgery (CSRF) vulnerability in Web UI of Secomea GateManager allows phishing attacker to issue get request in logged in user session.	4.2	More Details
CVE-2022-24466	Windows Hyper-V Security Feature Bypass Vulnerability	4.1	More Details
CVE-2022-29423	Pro Features Lock Bypass vulnerability in Countdown & Clock plugin <= 2.3.2 at WordPress.	3.8	More Details
CVE-2022-1590	A vulnerability was found in Bludit 3.13.1. It has been declared as problematic. This vulnerability affects the endpoint /admin/new-content of the New Content module. The manipulation of the argument content with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely but requires an authentication. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-30130	.NET Framework Denial of Service Vulnerability	3.3	More Details
CVE-2022-28162	Brocade SANnav before version SANnav 2.2.0 logs the REST API Authentication token in plain text.	3.3	More Details
CVE-2022-24099	Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (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.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1389	On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP (fixed in 17.0.0), a cross-site request forgery (CSRF) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. This vulnerability allows an attacker to run a limited set of commands: ping, traceroute, and WOM diagnostics. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	3.1	More Details
CVE-2022-24902	TkVideoplayer is a simple library to play video files in tkinter. Uncontrolled memory consumption in versions of TKVideoplayer prior to 2.0.0 can theoretically lead to performance degradation. There are no known workarounds. This issue has been patched and users are advised to upgrade to version 2.0.0 or later.	2.9	More Details
CVE-2021-27759	This vulnerability arises because the application allows the user to perform some sensitive action without verifying that the request was sent intentionally. An attacker can cause a victim's browser to emit an HTTP request to an arbitrary URL in the application.	2.3	More Details
CVE-2022-28274	Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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.	N/A	More Details
CVE-2022-28273	Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28272	Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28271	Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (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 PDF file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28270	Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28279	Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (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-2022-28275	Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-23205	Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (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-2022-30294	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-30293. Reason: This candidate is a duplicate of CVE-2022-30293. Notes: All CVE users should reference CVE-2022-30293 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-28276	Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-29175	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: None. Reason: This candidate was withdrawn. Further investigation showed that it was not a security issue. Notes: Consult https://github.com/vyperlang/vyper/security/advisories/GHSA-42j8-8cjv-j5r9 for more information. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28277	Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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 PDF file.	N/A	More Details
CVE-2022-1588	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-28066	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-26280. Reason: This candidate is a duplicate of CVE-2022-26280. Notes: All CVE users should reference CVE-2022-26280 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-24105	Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (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 U3D file.	N/A	More Details