SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 19 October 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-2022-35698	Adobe Commerce versions 2.4.4-p1 (and earlier) and 2.4.5 (and earlier) are affected by a Stored Cross-site Scripting vulnerability. Exploitation of this issue does not require user interaction and could result in a post-authentication arbitrary code execution.	10.0	More Details
CVE-2020-8974	In ZGR TPS200 NG 2.00 firmware version and 1.01 hardware version, the firmware upload process does not perform any type of restriction. This allows an attacker to modify it and re-upload it via web with malicious modifications, rendering the device unusable.	10.0	More Details
CVE-2022-2884	A vulnerability in GitLab CE/EE affecting all versions from 11.3.4 prior to 15.1.5, 15.2 to 15.2.3, 15.3 to 15.3 to 15.3.1 allows an an authenticated user to achieve remote code execution via the Import from GitHub API endpoint	9.9	More Details
CVE-2022-2992	A vulnerability in GitLab CE/EE affecting all versions from 11.10 prior to 15.1.6, 15.2 to 15.2.4, 15.3 to 15.3.2 allows an authenticated user to achieve remote code execution via the Import from GitHub API endpoint.	9.9	More Details
CVE-2022-42171	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/saveParentControlInfo.	9.8	More Details
CVE-2022-42169	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/addWifiMacFilter.	9.8	More Details
CVE-2022-42168	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/fromSetIpMacBind.	9.8	More Details
CVE-2022-42167	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetFirewallCfg.	9.8	More Details
CVE-2022-42166	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetSpeedWan.	9.8	More Details
CVE-2022-42154	An arbitrary file upload vulnerability in the component /apiadmin/upload/attach of 74cmsSE v3.13.0 allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details
CVE-2022-42165	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetDeviceName.	9.8	More Details
CVE-2022-42164	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetClientState.	9.8	More Details
CVE-2022-42163	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/fromNatStaticSetting.	9.8	More Details
CVE-2022-2052	Multiple Trumpf Products in multiple versions use default privileged Windows users and passwords. An adversary may use these accounts to remotely gain full access to the system.	9.8	More Details
CVE-2022-42980	go-admin (aka GO Admin) 2.0.12 uses the string go-admin as a production JWT key.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42968	Gitea before 1.17.3 does not sanitize and escape refs in the git backend. Arguments to git commands are mishandled.	9.8	More Details
CVE-2017-20149	The Mikrotik RouterOS web server allows memory corruption in releases before Stable 6.38.5 and Long-term 6.37.5, aka Chimay-Red. A remote and unauthenticated user can trigger the vulnerability by sending a crafted HTTP request. An attacker can use this vulnerability to execute arbitrary code on the affected system, as exploited in the wild in mid-2017 and later.	9.8	More Details
CVE-2022-38418	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction.	9.8	More Details
CVE-2022-37611	Prototype pollution vulnerability in tschaub gh-pages 3.1.0 via the partial variable in util.js.	9.8	More Details
CVE-2022-42170	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formWifiWpsStart.	9.8	More Details
CVE-2022-41408	Online Pet Shop We App v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=orders/view_order.	9.8	More Details
CVE-2022-42237	A SQL Injection issue in Merchandise Online Store v.1.0 allows an attacker to log in to the admin account.	9.8	More Details
CVE-2022-35711	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, the vulnerability is triggered when a crafted network packet is sent to the server.	9.8	More Details
CVE-2022-22128	Tableau discovered a path traversal vulnerability affecting Tableau Server Administration Agent's internal file transfer service that could allow remote code execution.Tableau only supports product versions for 24 months after release. Older versions have reached their End of Life and are no longer supported. They are also not assessed for potential security issues and do not receive security updates.	9.8	More Details
CVE-2022-40055	An issue in GX Group GPON ONT Titanium 2122A T2122-V1.26EXL allows attackers to escalate privileges via a brute force attack at the login page.	9.8	More Details
CVE-2022-42149	kkFileView 4.0 is vulnerable to Server-side request forgery (SSRF) via controller\OnlinePreviewController.java.	9.8	More Details
CVE-2022-39056	RAVA certificate validation system has insufficient validation for user input. An unauthenticated remote attacker can inject arbitrary SQL command to access, modify and delete database.	9.8	More Details
CVE-2022-31122	Wire is an encrypted communication and collaboration platform. Versions prior to 2022-07-12/Chart 4.19.0 are subject to Token Recipient Confusion. If an attacker has certain details of SAML IdP metadata, and configures their own SAML on the same backend, the attacker can delete all SAML authenticated accounts of a targeted team, Authenticate as a user of the attacked team and create arbitrary accounts in the context of the team if it is not managed by SCIM. This issue is fixed in wire-server 2022-07-12 and is already deployed on all Wire managed services. On-premise instances of wire-server need to be updated to 2022-07-12/Chart 4.19.0, so that their backends are no longer affected. As a workaround, the risk of an attack can be reduced by disabling SAML configuration for teams (galley.config.settings.featureFlags.sso). Helm overrides are located in `values/wire-server/values.yaml` Note that the ability to configure SAML SSO as a team is disabled by default for on-premise installations.	9.8	More Details
CVE-2022-40889	Phpok 6.1 has a deserialization vulnerability via framework/phpok_call.php.	9.8	More Details
CVE-2022-40684	An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.	9.8	More Details
CVE-2022-33872	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in Telnet login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated remote attacker to execute arbitrary command in the underlying shell.	9.8	More Details
CVE-2022-33874	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in SSH login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated remote attacker to execute arbitrary command in the underlying shell.	9.8	More Details
CVE-2022-41544	GetSimple CMS v3.3.16 was discovered to contain a remote code execution (RCE) vulnerability via the edited_file parameter in admin/theme-edit.php.	9.8	More Details
CVE-2022-43260	Tenda AC18 V15.03.05.19(6318) was discovered to contain a stack overflow via the time parameter in the fromSetSysTime function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39198	A deserialization vulnerability existed in dubbo hessian-lite 3.2.12 and its earlier versions, which could lead to malicious code execution. This issue affects Apache Dubbo 2.7.x version 2.7.17 and prior versions; Apache Dubbo 3.0.x version 3.0.11 and prior versions; Apache Dubbo 3.1.x version 3.1.0 and prior versions.	9.8	More Details
CVE-2022-21587	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: Upload). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks of this vulnerability can result in takeover of Oracle Web Applications Desktop Integrator. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2022-0699	A double-free condition exists in contrib/shpsort.c of shapelib 1.5.0 and older releases. This issue may allow an attacker to cause a denial of service or have other unspecified impact via control over malloc.	9.8	More Details
CVE-2022-35712	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, the vulnerability is triggered when a crafted network packet is sent to the server.	9.8	More Details
CVE-2022-35710	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, the vulnerability is triggered when a crafted network packet is sent to the server.	9.8	More Details
CVE-2022-41390	OcoMon v4.0 was discovered to contain a SQL injection vulnerability via the cod parameter at download.php.	9.8	More Details
CVE-2022-41496	iCMS v7.0.16 was discovered to contain a Server-Side Request Forgery (SSRF) via the url parameter at admincp.php.	9.8	More Details
CVE-2022-41495	ClipperCMS 1.3.3 was discovered to contain a Server-Side Request Forgery (SSRF) via the rss_url_news parameter at /manager/index.php.	9.8	More Details
CVE-2022-3457	Origin Validation Error in GitHub repository ikus060/rdiffweb prior to 2.5.0a5.	9.8	More Details
CVE-2022-3456	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.5.0.	9.8	More Details
CVE-2022-42889	Apache Commons Text performs variable interpolation, allowing properties to be dynamically evaluated and expanded. The standard format for interpolation is "${prefix:name}", where "prefix" is used to locate an instance of org.apache.commons.text.lookup.StringLookup that performs the interpolation. Starting with version 1.5 and continuing through 1.9, the set of default Lookup instances included interpolators that could result in arbitrary code execution or contact with remote servers. These lookups are: - "script" - execute expressions using the JVM script execution engine (javax.script) - "dns" - resolve dns records - "url" - load values from urls, including from remote servers Applications using the interpolation defaults in the affected versions may be vulnerable to remote code execution or unintentional contact with remote servers if untrusted configuration values are used. Users are recommended to upgrade to Apache Commons Text 1.10.0, which disables the problematic interpolators by default.	9.8	More Details
CVE-2022-24697	Kylin's cube designer function has a command injection vulnerability when overwriting system parameters in the configuration overwrites menu. RCE can be implemented by closing the single quotation marks around the parameter value of “-- conf=” to inject any operating system command into the command line parameters. This vulnerability affects Kylin 2 version 2.6.5 and earlier, Kylin 3 version 3.1.2 and earlier, and Kylin 4 version 4.0.1 and earlier.	9.8	More Details
CVE-2022-42897	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected.	9.8	More Details
CVE-2018-18447	dotPDN Paint.NET before 4.1.2 allows Deserialization of Untrusted Data (issue 2 of 2).	9.8	More Details
CVE-2018-18446	dotPDN Paint.NET before 4.1.2 allows Deserialization of Untrusted Data (issue 1 of 2).	9.8	More Details
CVE-2022-37601	Prototype pollution vulnerability in function parseQuery in parseQuery.js in webpack loader-utils via the name variable in parseQuery.js. This affects all versions prior to 1.4.1 and 2.0.3.	9.8	More Details
CVE-2022-41403	OpenCart 3.x Newsletter Custom Popup was discovered to contain a SQL injection vulnerability via the email parameter at index.php?route=extension/module/so_newletter_custom_popup/newsletter.	9.8	More Details
CVE-2022-33106	WiJungle NGFW Version U250 was discovered to be vulnerable to No Rate Limit attack, allowing the attacker to brute force the admin password leading to Account Take Over.	9.8	More Details
CVE-2022-40871	Dolibarr ERP & CRM <=15.0.3 is vulnerable to Eval injection. By default, any administrator can be added to the installation page of dolibarr, and if successfully added, malicious code can be inserted into the database and then execute it by eval.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37614	Prototype pollution vulnerability in function enable in mockery.js in mfncooper mockery commit 822f0566fd6d72af8c943ae5ca2aa92e516aa2cf via the key variable in mockery.js.	9.8	More Details
CVE-2022-40664	Apache Shiro before 1.10.0, Authentication Bypass Vulnerability in Shiro when forwarding or including via RequestDispatcher.	9.8	More Details
CVE-2022-35690	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, the vulnerability is triggered when a crafted network packet is sent to the server.	9.8	More Details
CVE-2022-41497	ClipperCMS 1.3.3 was discovered to contain a Server-Side Request Forgery (SSRF) via the pkg_url parameter at /manager/index.php.	9.8	More Details
CVE-2022-41391	OcoMon v4.0 was discovered to contain a SQL injection vulnerability via the cod parameter at showImg.php.	9.8	More Details
CVE-2022-38980	The HwAirlink module has a heap overflow vulnerability in processing data packets of the proprietary protocol.Successful exploitation of this vulnerability may allow attackers to obtain process control permissions.	9.8	More Details
CVE-2022-41580	The HW_KEYMASTER module has a vulnerability of not verifying the data read.Successful exploitation of this vulnerability may cause malicious construction of data, which results in out-of-bounds access.	9.8	More Details
CVE-2022-41578	The MPTCP module has an out-of-bounds write vulnerability.Successful exploitation of this vulnerability may cause root privilege escalation attacks implemented by modifying program information.	9.8	More Details
CVE-2022-38983	The BT Hfp Client module has a Use-After-Free (UAF) vulnerability.Successful exploitation of this vulnerability may result in arbitrary code execution.	9.8	More Details
CVE-2022-38982	The fingerprint module has service logic errors.Successful exploitation of this vulnerability will cause the phone lock to be cracked.	9.8	More Details
CVE-2022-42064	Online Diagnostic Lab Management System version 1.0 remote exploit that bypasses login with SQL injection and then uploads a shell.	9.8	More Details
CVE-2022-3439	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.5.0.	9.8	More Details
CVE-2022-37602	Prototype pollution vulnerability in karma-runner grunt-karma 4.0.1 via the key variable in grunt-karma.js.	9.8	More Details
CVE-2022-39428	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: Upload). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks of this vulnerability can result in takeover of Oracle Web Applications Desktop Integrator. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-8976	The integrated server of the ZGR TPS200 NG on its 2.00 firmware version and 1.01 hardware version, allows a remote attacker to perform actions with the permissions of a victim user. For this to happen, the victim user has to have an active session and triggers the malicious request.	9.6	More Details
CVE-2022-42711	In Progress WhatsUp Gold before 22.1.0, an SNMP MIB Walker application endpoint failed to adequately sanitize malicious input. This could allow an unauthenticated attacker to execute arbitrary code in a victim's browser.	9.6	More Details
CVE-2020-8973	ZGR TPS200 NG in its 2.00 firmware version and 1.01 hardware version, does not properly accept specially constructed requests. This allows an attacker with access to the network where the affected asset is located, to operate and change several parameters without having to be registered as a user on the web that owns the device.	9.3	More Details
CVE-2021-46840	The HW_KEYMASTER module has an out-of-bounds access vulnerability in parameter set verification.Successful exploitation of this vulnerability may cause malicious construction of data, which results in out-of-bounds access.	9.1	More Details
CVE-2021-46839	The HW_KEYMASTER module has a vulnerability of missing bounds check on length.Successful exploitation of this vulnerability may cause malicious construction of data, which results in out-of-bounds access.	9.1	More Details
CVE-2022-38986	The HIPP module has a vulnerability of bypassing the check of the data transferred in the kernel space.Successful exploitation of this vulnerability may cause out-of-bounds access to the HIPP module and page table tampering, affecting device confidentiality and availability.	9.1	More Details
CVE-2022-41581	The HW_KEYMASTER module has a vulnerability of not verifying the data read.Successful exploitation of this vulnerability may cause malicious construction of data, which results in out-of-bounds access.	9.1	More Details
CVE-2022-41436	An issue in OXHOO TP50 OXH1.50 allows unauthenticated attackers to access the administrative panel via browsing to the URL http://device_ip/index1.html.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39311	GoCD is a continuous delivery server. GoCD helps you automate and streamline the build-test-release cycle for continuous delivery of your product. GoCD versions prior to 21.1.0 are vulnerable to remote code execution on the server from a malicious or compromised agent. The Spring RemoteInvocation endpoint exposed agent communication and allowed deserialization of arbitrary java objects, as well as subsequent remote code execution. Exploitation requires agent-level authentication, thus an attacker would need to either compromise an existing agent, its network communication or register a new agent to practically exploit this vulnerability. This issue is fixed in GoCD version 21.1.0. There are currently no known workarounds.	9.1	More Details
CVE-2022-41477	A security issue was discovered in WeBid <=1.2.2. A Server-Side Request Forgery (SSRF) vulnerability in the admin/theme.php file allows remote attackers to inject payloads via theme parameters to read files across directories.	9.1	More Details
CVE-2022-32176	In "Gin-Vue-Admin", versions v2.5.1 through v2.5.3b are vulnerable to Unrestricted File Upload that leads to execution of javascript code, through the "Compress Upload" functionality to the Media Library. When an admin user views the uploaded file, a low privilege attacker will get access to the admin's cookie leading to account takeover.	9.0	More Details
CVE-2022-32177	In "Gin-Vue-Admin", versions v2.5.1 through v2.5.3beta are vulnerable to Unrestricted File Upload that leads to execution of javascript code, through the 'Normal Upload' functionality to the Media Library. When an admin user views the uploaded file, a low privilege attacker will get access to the admin’s cookie leading to account takeover.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-28866	Multiple Improper Access Control was discovered in Nokia AirFrame BMC Web GUI < R18 Firmware v4.13.00. It does not properly validate requests for access to (or editing of) data and functionality in all endpoints under /#settings/* and /api/settings/*. By not verifying the permissions for access to resources, it allows a potential attacker to view pages, with sensitive data, that are not allowed, and modify system configurations also causing DoS, which should be accessed only by user with administration profile, bypassing all controls (without checking for user identity).	8.8	More Details
CVE-2022-42070	Online Birth Certificate Management System version 1.0 is vulnerable to Cross Site Request Forgery (CSRF).	8.8	More Details
CVE-2022-37208	JFinal CMS 5.1.0 is vulnerable to SQL Injection. These interfaces do not use the same component, nor do they have filters, but each uses its own SQL concatenation method, resulting in SQL injection.	8.8	More Details
CVE-2022-41475	RPCMS v3.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily add an administrator account.	8.8	More Details
CVE-2022-42156	D-Link COVR 1200,1203 v1.08 was discovered to contain a command injection vulnerability via the tomography_ping_number parameter at function SetNetworkTomographySettings.	8.8	More Details
CVE-2022-42160	D-Link COVR 1200,1202,1203 v1.08 was discovered to contain a command injection vulnerability via the system_time_timezone parameter at function SetNTPServerSettings.	8.8	More Details
CVE-2022-42161	D-Link COVR 1200,1202,1203 v1.08 was discovered to contain a command injection vulnerability via the /SetTriggerWPS/PIN parameter at function SetTriggerWPS.	8.8	More Details
CVE-2022-35135	Boodskap IoT Platform v4.4.9-02 allows attackers to escalate privileges via a crafted request sent to /api/user/upsert/<uuid>.	8.8	More Details
CVE-2022-42719	A use-after-free in the mac80211 stack when parsing a multi-BSSID element in the Linux kernel 5.2 through 5.19.x before 5.19.16 could be used by attackers (able to inject WLAN frames) to crash the kernel and potentially execute code.	8.8	More Details
CVE-2022-36803	The MasterUserEdit API in Atlassian Jira Align Server before version 10.109.2 allows An authenticated attacker with the People role permission to use the MasterUserEdit API to modify any users role to Super Admin. This vulnerability was reported by Jacob Shafer from Bishop Fox.	8.8	More Details
CVE-2022-41538	Wedding Planner v1.0 was discovered to contain an arbitrary file upload vulnerability in the component /Wedding-Management-PHP/admin/photos_add.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41539	Wedding Planner v1.0 was discovered to contain an arbitrary file upload vulnerability in the component /admin/users_add.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	8.8	More Details
CVE-2021-27406	An attacker can take leverage on PerFact OpenVPN-Client versions 1.4.1.0 and prior to send the config command from any application running on the local host machine to force the back-end server into initializing a new open-VPN instance with arbitrary open-VPN configuration. This could result in the attacker achieving execution with privileges of a SYSTEM user.	8.8	More Details
CVE-2022-34020	Cross Site Request Forgery (CSRF) vulnerability in ResIOT ResIOT IOT Platform + LoRaWAN Network Server through 4.1.1000114 allows attackers to add new admin users to the platform or other unspecified impacts.	8.8	More Details
CVE-2022-42234	There is a file inclusion vulnerability in the template management module in UCMS 1.6	8.8	More Details
CVE-2022-42983	anji-plus AJ-Report 0.9.8.6 allows remote attackers to bypass login authentication by spoofing JWT Tokens.	8.8	More Details
CVE-2019-14841	A flaw was found in the RHDM, where an authenticated attacker can change their assigned role in the response header. This flaw allows an attacker to gain admin privileges in the Business Central Console.	8.8	More Details
CVE-2022-23770	This vulnerability could allow a remote attacker to execute remote commands with improper validation of parameters of certain API constructors. Remote attackers could use this vulnerability to execute malicious commands such as directory traversal.	8.8	More Details
CVE-2022-42221	Netgear R6220 v1.1.0.114_1.0.1 suffers from Incorrect Access Control, resulting in a command injection vulnerability.	8.8	More Details
CVE-2022-42029	Chamilo 1.11.16 is affected by an authenticated local file inclusion vulnerability which allows authenticated users with access to 'big file uploads' to copy/move files from anywhere in the file system into the web directory.	8.8	More Details
CVE-2022-38743	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an improper access control vulnerability. The FactoryTalk VantagePoint SQL Server account could allow a malicious user with read-only privileges to execute SQL statements in the back-end database. If successfully exploited, this could allow the attacker to execute arbitrary code and gain access to restricted data.	8.8	More Details
CVE-2022-3158	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an input validation vulnerability. The FactoryTalk VantagePoint SQL Server lacks input validation when users enter SQL statements to retrieve information from the back-end database. If successfully exploited, this could allow a user with basic user privileges to perform remote code execution on the server.	8.8	More Details
CVE-2022-21613	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Data Quality, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data as well as unauthorized update, insert or delete access to some of Oracle Enterprise Data Quality accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Data Quality. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:L).	8.8	More Details
CVE-2022-39427	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	8.8	More Details
CVE-2022-42902	In Linaro Automated Validation Architecture (LAVA) before 2022.10, there is dynamic code execution in lava_server/lavatable.py. Due to improper input sanitization, an anonymous user can force the lava-server-gunicorn service to execute user-provided code on the server.	8.8	More Details
CVE-2022-41500	EyouCMS V1.5.9 was discovered to contain multiple Cross-Site Request Forgery (CSRF) vulnerabilities via the Members Center, Editorial Membership, and Points Recharge components.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40469	iKuai OS v3.6.7 was discovered to contain an authenticated remote code execution (RCE) vulnerability.	8.8	More Details
CVE-2022-39293	Azure RTOS USBX is a high-performance USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. The case is, in [_ux_host_class_pima_read](https://github.com/azure-rtos/usbx/blob/master/common/usbx_host_classes/src/ux_host_class_pima_read.c), there is data length from device response, returned in the very first packet, and read by [L165 code](https://github.com/azure-rtos/usbx/blob/082fd9db09a3669eca3358f10b8837a5c1635c0b/common/usbx_host_classes/src/ux_host_class_pima_read.c#L165), as header_length. Then in [L178 code](https://github.com/azure-rtos/usbx/blob/082fd9db09a3669eca3358f10b8837a5c1635c0b/common/usbx_host_classes/src/ux_host_class_pima_read.c#L178), there is a “if” branch, which check the expression of “(header_length - UX_HOST_CLASS_PIMA_DATA_HEADER_SIZE) > data_length” where if header_length is smaller than UX_HOST_CLASS_PIMA_DATA_HEADER_SIZE, calculation could overflow and then [L182 code](https://github.com/azure-rtos/usbx/blob/082fd9db09a3669eca3358f10b8837a5c1635c0b/common/usbx_host_classes/src/ux_host_class_pima_read.c#L182) the calculation of data_length is also overflow, this way the later [while loop start from L192](https://github.com/azure-rtos/usbx/blob/082fd9db09a3669eca3358f10b8837a5c1635c0b/common/usbx_host_classes/src/ux_host_class_pima_read.c#L192) can move data_pointer to unexpected address and cause write buffer overflow. The fix has been included in USBX release [6.1.12](https://github.com/azure-rtos/usbx/releases/tag/v6.1.12_rel). The following can be used as a workaround: Add check of `header_length`: 1. It must be greater than `UX_HOST_CLASS_PIMA_DATA_HEADER_SIZE`. 1. It should be greater or equal to the current returned data length (`transfer_request -> ux_transfer_request_actual_length`).	8.6	More Details
CVE-2022-42488	OpenHarmony-v3.1.2 and prior versions have a Missing permission validation vulnerability in param service of startup subsystem. An malicious application installed on the device could elevate its privileges to the root user, disable security features, or cause DoS by disabling particular services.	8.4	More Details
CVE-2022-22229	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability, a stored XSS (or persistent), in the Control Center Controller web pages of Juniper Networks Paragon Active Assurance (Formerly Netrounds) allows a high-privilege attacker with 'WRITE' permissions to store one or more malicious scripts that will infect any other authorized user's account when they accidentally trigger the malicious script(s) while managing the device. Triggering these attacks enables the attacker to execute commands with the permissions up to that of the superuser account. This issue affects: Juniper Networks Paragon Active Assurance (Formerly Netrounds) All versions prior to 3.1.1; 3.2 versions prior to 3.2.1.	8.4	More Details
CVE-2022-42463	OpenHarmony-v3.1.2 and prior versions have an authenication bypass vulnerability in a callback handler function of Softbus_server in communication subsystem. Attackers can launch attacks on distributed networks by sending Bluetooth rfcomm packets to any remote device and executing arbitrary commands.	8.3	More Details
CVE-2022-32488	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	8.2	More Details
CVE-2022-32489	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	8.2	More Details
CVE-2022-28759	Zoom On-Premise Meeting Connector MMR before version 4.8.20220815.130 contains an improper access control vulnerability. As a result, a malicious actor could obtain the audio and video feed of a meeting they were not authorized to join and cause other meeting disruptions.	8.2	More Details
CVE-2022-22239	An Execution with Unnecessary Privileges vulnerability in Management Daemon (mgd) of Juniper Networks Junos OS Evolved allows a locally authenticated attacker with low privileges to escalate their privileges on the device and potentially remote systems. This vulnerability allows a locally authenticated attacker with access to the ssh operational command to escalate their privileges on the system to root, or if there is user interaction on the local device to potentially escalate privileges on a remote system to root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-EVO; 21.2-EVO versions prior to 21.2R2-S1-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS.	8.2	More Details
CVE-2022-22241	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2.	8.1	More Details
CVE-2022-41489	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the affected device. This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31228	Dell EMC XtremIO versions prior to X2 6.4.0-22 contain a bruteforce vulnerability. A remote unauthenticated attacker can potentially exploit this vulnerability and gain access to an admin account.	8.1	More Details
CVE-2022-39064	An attacker sending a single malformed IEEE 802.15.4 (Zigbee) frame makes the TRÅDFRI bulb blink, and if they replay (i.e. resend) the same frame multiple times, the bulb performs a factory reset. This causes the bulb to lose configuration information about the Zigbee network and current brightness level. After this attack, all lights are on with full brightness, and a user cannot control the bulbs with either the IKEA Home Smart app or the TRÅDFRI remote control. The malformed Zigbee frame is an unauthenticated broadcast message, which means all vulnerable devices within radio range are affected. CVSS 3.1 Base Score 7.1 vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	8.1	More Details
CVE-2022-2780	In affected versions of Octopus Server it is possible to use the Git Connectivity test function on the VCS project to initiate an SMB request resulting in the potential for an NTLM relay attack.	8.1	More Details
CVE-2022-39303	Ree6 is a moderation bot. This vulnerability allows manipulation of SQL queries. This issue has been patched in version 1.7.0 by using Javas PreparedStatements, which allow object setting without the risk of SQL injection. There are currently no known workarounds.	8.1	More Details
CVE-2022-0030	An authentication bypass vulnerability in the Palo Alto Networks PAN-OS 8.1 web interface allows a network-based attacker with specific knowledge of the target firewall or Panorama appliance to impersonate an existing PAN-OS administrator and perform privileged actions.	8.1	More Details
CVE-2022-41541	TP-Link AX10v1 V1_211117 allows attackers to execute a replay attack by using a previously transmitted encrypted authentication message and valid authentication token. Attackers are able to login to the web application as an admin user.	8.1	More Details
CVE-2022-39424	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Difficult to exploit vulnerability allows unauthenticated attacker with network access via VRDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2022-39426	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Difficult to exploit vulnerability allows unauthenticated attacker with network access via VRDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2022-21612	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Data Quality accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2022-39406	Vulnerability in the PeopleSoft Enterprise Common Components product of Oracle PeopleSoft (component: Approval Framework). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise Common Components. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise Common Components accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise Common Components accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2022-35846	An improper restriction of excessive authentication attempts vulnerability [CWE-307] in FortiTester Telnet port 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated attacker to guess the credentials of an admin user via a brute force attack.	8.1	More Details
CVE-2022-41674	An issue was discovered in the Linux kernel before 5.19.16. Attackers able to inject WLAN frames could cause a buffer overflow in the ieee80211_bss_info_update function in net/mac80211/scan.c.	8.1	More Details
CVE-2022-39425	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Difficult to exploit vulnerability allows unauthenticated attacker with network access via VRDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2022-23771	This vulnerability occurs in user accounts creation and deleteion related pages of IPTIME NAS products. The vulnerability could be exploited by a lack of validation when a POST request is made to this page. An attacker can use this vulnerability to or delete user accounts, or to escalate arbitrary user privileges.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40187	Foresight GC3 Launch Monitor 1.3.15.68 ships with a Target Communication Framework (TCF) service enabled. This service listens on a TCP port on all interfaces and allows for process debugging, file system modification, and terminal access as the root user. In conjunction with a hosted wireless access point and the known passphrase of FSSPORTS, an attacker could use this service to modify a device and steal intellectual property.	8.0	More Details
CVE-2022-41307	A maliciously crafted PKT file when consumed through SubassemblyComposer.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-41306	A maliciously crafted PCT file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-41305	A maliciously crafted PKT file when consumed through SubassemblyComposer.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-41304	An Out-Of-Bounds Write Vulnerability in Autodesk FBX SDK 2020 version and prior may lead to code execution through maliciously crafted FBX files or information disclosure.	7.8	More Details
CVE-2022-41303	A user may be tricked into opening a malicious FBX file which may exploit a use-after-free vulnerability in Autodesk FBX SDK 2020 version causing the application to reference a memory location controlled by an unauthorized third party, thereby running arbitrary code on the system.	7.8	More Details
CVE-2022-41302	An Out-Of-Bounds Read Vulnerability in Autodesk FBX SDK version 2020. and prior may lead to code execution or information disclosure through maliciously crafted FBX files. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2021-0699	In HTBLogKM of TBD, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-242345178	7.8	More Details
CVE-2022-20397	In SitRilClient_OnResponse of SitRilSe.cpp, 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-223086933References: N/A	7.8	More Details
CVE-2022-42720	Various refcounting bugs in the multi-BSS handling in the mac80211 stack in the Linux kernel 5.1 through 5.19.x before 5.19.16 could be used by local attackers (able to inject WLAN frames) to trigger use-after-free conditions to potentially execute code.	7.8	More Details
CVE-2022-41585	The kernel module has an out-of-bounds read vulnerability.Successful exploitation of this vulnerability may cause memory overwriting.	7.8	More Details
CVE-2022-41584	The kernel module has an out-of-bounds read vulnerability.Successful exploitation of this vulnerability may cause memory overwriting.	7.8	More Details
CVE-2022-41576	The rphone module has a script that can be maliciously modified.Successful exploitation of this vulnerability may cause irreversible programs to be implanted on user devices.	7.8	More Details
CVE-2022-2985	In music service, there is a missing permission check. This could lead to elevation of privilege in contacts service with no additional execution privileges needed.	7.8	More Details
CVE-2022-41308	A maliciously crafted PKT file when consumed through SubassemblyComposer.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-42339	Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by a Stack-based Buffer Overflow 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-2022-38669	In soundrecorder service, there is a missing permission check. This could lead to elevation of privilege in contacts service with no additional execution privileges needed.	7.8	More Details
CVE-2022-38670	In soundrecorder service, there is a missing permission check. This could lead to elevation of privilege in contacts service with no additional execution privileges needed.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36438	AsusSwitch.exe on ASUS personal computers (running Windows) sets weak file permissions, leading to local privilege escalation (this also can be used to delete files within the system arbitrarily). This affects ASUS System Control Interface 3 before 3.1.5.0, and AsusSwitch.exe before 1.0.10.0.	7.8	More Details
CVE-2021-3305	Beijing Feishu Technology Co., Ltd Feishu v3.40.3 was discovered to contain an untrusted search path vulnerability.	7.8	More Details
CVE-2022-22251	On cSRX Series devices software permission issues in the container filesystem and stored files combined with storing passwords in a recoverable format in Juniper Networks Junos OS allows a local, low-privileged attacker to elevate their permissions to take control of any instance of a cSRX software deployment. This issue affects Juniper Networks Junos OS 20.2 version 20.2R1 and later versions prior to 21.2R1 on cSRX Series.	7.8	More Details
CVE-2022-3569	Due to an issue with incorrect sudo permissions, Zimbra Collaboration Suite (ZCS) suffers from a local privilege escalation issue in versions 9.0.0 and prior, where the 'zimbra' user can effectively coerce postfix into running arbitrary commands as 'root'.	7.8	More Details
CVE-2022-41751	Jhead 3.06.0.1 allows attackers to execute arbitrary OS commands by placing them in a JPEG filename and then using the regeneration -rgt50 option.	7.8	More Details
CVE-2022-38450	Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by a Stack-based Buffer Overflow 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-2022-38448	Adobe Dimension versions 3.4.5 is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-38447	Adobe Dimension versions 3.4.5 is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-38446	Adobe Dimension versions 3.4.5 is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-38445	Adobe Dimension versions 3.4.5 is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-38444	Adobe Dimension versions 3.4.5 is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-38441	Adobe Dimension versions 3.4.5 is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-38440	Adobe Dimension versions 3.4.5 is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-39110	In Music service, there is a missing permission check. This could lead to elevation of privilege in Music service with no additional execution privileges needed.	7.8	More Details
CVE-2022-39109	In Music service, there is a missing permission check. This could lead to elevation of privilege in Music service with no additional execution privileges needed.	7.8	More Details
CVE-2022-39108	In Music service, there is a missing permission check. This could lead to elevation of privilege in Music service with no additional execution privileges needed.	7.8	More Details
CVE-2022-39107	In Soundrecorder service, there is a missing permission check. This could lead to elevation of privilege in Soundrecorder service with no additional execution privileges needed.	7.8	More Details
CVE-2022-39080	In messaging service, there is a missing permission check. This could lead to elevation of privilege in contacts service with no additional execution privileges needed.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38698	In messaging service, there is a missing permission check. This could lead to elevation of privilege in contacts service with no additional execution privileges needed.	7.8	More Details
CVE-2022-39111	In Music service, there is a missing permission check. This could lead to elevation of privilege in Music service with no additional execution privileges needed.	7.8	More Details
CVE-2022-38442	Adobe Dimension versions 3.4.5 is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-42901	Bentley MicroStation and MicroStation-based applications may be affected by out-of-bounds and stack overflow issues when opening crafted XMT files. Exploiting these issues could lead to information disclosure and code execution. The fixed versions are 10.17.01.58* for MicroStation and 10.17.01.19* for Bentley View.	7.8	More Details
CVE-2022-42900	Bentley MicroStation and MicroStation-based applications may be affected by out-of-bounds read issues when opening crafted FBX files. Exploiting these issues could lead to information disclosure and code execution. The fixed versions are 10.17.01.58* for MicroStation and 10.17.01.19* for Bentley View.	7.8	More Details
CVE-2022-42899	Bentley MicroStation and MicroStation-based applications may be affected by out-of-bounds read and stack overflow issues when opening crafted SKP files. Exploiting these issues could lead to information disclosure and code execution. The fixed versions are 10.17.01.58* for MicroStation and 10.17.01.19* for Bentley View.	7.8	More Details
CVE-2022-33919	Dell GeoDrive, versions 2.1 - 2.2, contains an information disclosure vulnerability in GUI. An authenticated non-admin user could potentially exploit this vulnerability and view sensitive information.	7.8	More Details
CVE-2022-42906	powerline-gitstatus (aka Powerline Gitstatus) before 1.3.2 allows arbitrary code execution. git repositories can contain per-repository configuration that changes the behavior of git, including running arbitrary commands. When using powerline-gitstatus, changing to a directory automatically runs git commands in order to display information about the current repository in the prompt. If an attacker can convince a user to change their current directory to one controlled by the attacker, such as in a shared filesystem or extracted archive, powerline-gitstatus will run arbitrary commands under the attacker's control. NOTE: this is similar to CVE-2022-20001.	7.8	More Details
CVE-2022-33920	Dell GeoDrive, versions prior to 2.2, contains an Unquoted File Path vulnerability. A low privilege attacker could potentially exploit this vulnerability, leading to the execution of arbitrary code in the SYSTEM security context.	7.8	More Details
CVE-2022-39297	MelisCms provides a full CMS for Melis Platform, including templating system, drag'n'drop of plugins, SEO and many administration tools. Attackers can deserialize arbitrary data on affected versions of `melisplatform/melis-cms`, and ultimately leads to the execution of arbitrary PHP code on the system. Conducting this attack does not require authentication. Users should immediately upgrade to `melisplatform/melis-cms` >= 5.0.1. This issue was addressed by restricting allowed classes when deserializing user-controlled data.	7.7	More Details
CVE-2022-2249	Privilege escalation related vulnerabilities were discovered in Avaya Aura Communication Manager that may allow local administrative users to escalate their privileges. This issue affects Communication Manager versions 8.0.0.0 through 8.1.3.3 and 10.1.0.0.	7.7	More Details
CVE-2022-39300	node SAML is a SAML 2.0 library based on the SAML implementation of passport-saml. A remote attacker may be able to bypass SAML authentication on a website using passport-saml. A successful attack requires that the attacker is in possession of an arbitrary IDP signed XML element. Depending on the IDP used, fully unauthenticated attacks (e.g without access to a valid user) might also be feasible if generation of a signed message can be triggered. Users should upgrade to node-saml version 4.0.0-beta5 or newer. Disabling SAML authentication may be done as a workaround.	7.7	More Details
CVE-2022-39298	MelisFront is the engine that displays website hosted on Melis Platform. It deals with showing pages, plugins, URL rewritting, search optimization and SEO, etc. Attackers can deserialize arbitrary data on affected versions of `melisplatform/melis-front`, and ultimately leads to the execution of arbitrary PHP code on the system. Conducting this attack does not require authentication. Users should immediately upgrade to `melisplatform/melis-front` >= 5.0.1. This issue was addressed by restricting allowed classes when deserializing user-controlled data.	7.7	More Details
CVE-2022-21590	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Core Formatting API). Supported versions that are affected are 5.9.0.0, 6.4.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	7.6	More Details
CVE-2022-38420	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by a Use of Hard-coded Credentials vulnerability that could result in application denial-of-service by gaining access to start/stop arbitrary services. Exploitation of this issue does not require user interaction.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38422	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in information disclosure. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2022-38419	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in arbitrary file system read. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2022-41623	Sensitive Data Exposure in Villatheme ALD - AliExpress Dropshipping and Fulfillment for WooCommerce premium plugin <= 1.1.0 on WordPress.	7.5	More Details
CVE-2022-42340	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary file system read. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2022-41323	In Django 3.2 before 3.2.16, 4.0 before 4.0.8, and 4.1 before 4.1.2, internationalized URLs were subject to a potential denial of service attack via the locale parameter, which is treated as a regular expression.	7.5	More Details
CVE-2022-21614	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2022-42975	socket/transport.ex in Phoenix before 1.6.14 mishandles check_origin wildcarding. NOTE: LiveView applications are unaffected by default because of the presence of a LiveView CSRF token.	7.5	More Details
CVE-2022-39052	An external attacker is able to send a specially crafted email (with many recipients) and trigger a potential DoS of the system	7.5	More Details
CVE-2022-3281	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	7.5	More Details
CVE-2022-21598	Vulnerability in the Siebel Core - DB Deployment and Configuration product of Oracle Siebel CRM (component: Repository Utilities). Supported versions that are affected are 22.8 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Core - DB Deployment and Configuration. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel Core - DB Deployment and Configuration accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2022-42341	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in arbitrary file system read. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2021-20030	SonicWall GMS is vulnerable to file path manipulation resulting that an unauthenticated attacker can gain access to web directory containing application's binaries and configuration files.	7.5	More Details
CVE-2022-43259	Tenda AC15 V15.03.05.18 was discovered to contain a stack overflow via the timeZone parameter in the form_fast_setting_wifi_set function.	7.5	More Details
CVE-2022-41582	The security module has configuration defects.Successful exploitation of this vulnerability may affect system availability.	7.5	More Details
CVE-2022-41715	Programs which compile regular expressions from untrusted sources may be vulnerable to memory exhaustion or denial of service. The parsed regexp representation is linear in the size of the input, but in some cases the constant factor can be as high as 40,000, making relatively small regexps consume much larger amounts of memory. After fix, each regexp being parsed is limited to a 256 MB memory footprint. Regular expressions whose representation would use more space than that are rejected. Normal use of regular expressions is unaffected.	7.5	More Details
CVE-2022-38981	The HwAirlink module has an out-of-bounds read vulnerability.Successful exploitation of this vulnerability may cause information leakage.	7.5	More Details
CVE-2022-32149	An attacker may cause a denial of service by crafting an Accept-Language header which ParseAcceptLanguage will take significant time to parse.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2880	Requests forwarded by ReverseProxy include the raw query parameters from the inbound request, including unparsable parameters rejected by net/http. This could permit query parameter smuggling when a Go proxy forwards a parameter with an unparsable value. After fix, ReverseProxy sanitizes the query parameters in the forwarded query when the outbound request's Form field is set after the ReverseProxy. Director function returns, indicating that the proxy has parsed the query parameters. Proxies which do not parse query parameters continue to forward the original query parameters unchanged.	7.5	More Details
CVE-2022-2879	Reader.Read does not set a limit on the maximum size of file headers. A maliciously crafted archive could cause Read to allocate unbounded amounts of memory, potentially causing resource exhaustion or panics. After fix, Reader.Read limits the maximum size of header blocks to 1 MiB.	7.5	More Details
CVE-2022-38984	The HIPP module has a vulnerability of not verifying the data transferred in the kernel space.Successful exploitation of this vulnerability will cause out-of-bounds read, which affects data confidentiality.	7.5	More Details
CVE-2022-38985	The facial recognition module has a vulnerability in input validation.Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-38998	The HISP module has a vulnerability of not verifying the data transferred in the kernel space.Successful exploitation of this vulnerability will cause out-of-bounds read, which affects data confidentiality.	7.5	More Details
CVE-2022-39011	The HISP module has a vulnerability of bypassing the check of the data transferred in the kernel space.Successful exploitation of this vulnerability may cause unauthorized access to the HISP module.	7.5	More Details
CVE-2022-41583	The storage maintenance and debugging module has an array out-of-bounds read vulnerability.Successful exploitation of this vulnerability will cause incorrect statistics of this module.	7.5	More Details
CVE-2022-2963	A vulnerability found in jasper. This security vulnerability happens because of a memory leak bug in function cmdopts_parse that can cause a crash or segmentation fault.	7.5	More Details
CVE-2022-21634	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: LLVM Interpreter). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2022-41586	The communication framework module has a vulnerability of not truncating data properly.Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-41588	The home screen module has a vulnerability in service logic processing.Successful exploitation of this vulnerability may affect data integrity.	7.5	More Details
CVE-2022-41589	The DFX unwind stack module of the ArkCompiler has a vulnerability in interface calling.Successful exploitation of this vulnerability affects system services and device availability.	7.5	More Details
CVE-2022-21623	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Application Config Console). Supported versions that are affected are 13.4.0.0 and 13.5.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2022-21622	Vulnerability in the Oracle SOA Suite product of Oracle Fusion Middleware (component: Adapters). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle SOA Suite accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2022-3479	A vulnerability found in nss. By this security vulnerability, nss client auth crash without a user certificate in the database and this can lead us to a segmentation fault or crash.	7.5	More Details
CVE-2022-42081	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 was discovered to contain a stack overflow via sched_end_time parameter.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21620	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2022-42188	In Lavalite 9.0.0, the XSRF-TOKEN cookie is vulnerable to path traversal attacks, enabling read access to arbitrary files on the server.	7.5	More Details
CVE-2019-14840	A flaw was found in the RHDM, where sensitive HTML form fields like Password has auto-complete enabled which may lead to leak of credentials.	7.5	More Details
CVE-2022-37603	A Regular expression denial of service (ReDoS) flaw was found in Function interpolateName in interpolateName.js in webpack loader-utils 2.0.0 via the url variable in interpolateName.js.	7.5	More Details
CVE-2022-22211	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO.	7.5	More Details
CVE-2022-41485	Tenda AC1200 US_AC6V2.0RTL_V15.03.06.51_multi_TDE01 was discovered to contain a buffer overflow in the 0x47ce00 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2022-41484	Tenda AC1900 AP500(US)_V1_180320(Beta) was discovered to contain a buffer overflow in the 0x32384 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2022-41483	Tenda AC1200 US_AC6V2.0RTL_V15.03.06.51_multi_TDE01 was discovered to contain a buffer overflow in the 0x4a12cc function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2022-41482	Tenda AC1200 US_AC6V2.0RTL_V15.03.06.51_multi_TDE01 was discovered to contain a buffer overflow in the 0x47c5dc function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2022-41481	Tenda AC1200 US_AC6V2.0RTL_V15.03.06.51_multi_TDE01 was discovered to contain a buffer overflow in the 0x47de1c function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2022-41480	Tenda AC1200 US_AC6V2.0RTL_V15.03.06.51_multi_TDE01 was discovered to contain a buffer overflow in the 0x475dc function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2022-22218	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22228	An Improper Validation of Specified Type of Input vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS allows an attacker to cause an RPD memory leak leading to a Denial of Service (DoS). This memory leak only occurs when the attacker's packets are destined to any configured IPv6 address on the device. This issue affects: Juniper Networks Junos OS 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1.	7.5	More Details
CVE-2022-39422	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.38. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2022-22231	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series if Unified Threat Management (UTM) Enhanced Content Filtering (CF) and AntiVirus (AV) are enabled together and the system processes specific valid transit traffic the Packet Forwarding Engine (PFE) will crash and restart. This issue affects Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1.	7.5	More Details
CVE-2022-32487	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	7.5	More Details
CVE-2022-32485	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	7.5	More Details
CVE-2022-22232	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1.	7.5	More Details
CVE-2022-22236	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1.	7.5	More Details
CVE-2022-34391	Dell Client BIOS Versions prior to the remediated version contain an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	7.5	More Details
CVE-2022-34390	Dell BIOS contains a use of uninitialized variable vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	7.5	More Details
CVE-2022-22246	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2.	7.5	More Details
CVE-2022-22247	An Improper Input Validation vulnerability in ingress TCP segment processing of Juniper Networks Junos OS Evolved allows a network-based unauthenticated attacker to send a crafted TCP segment to the device, triggering a kernel panic, leading to a Denial of Service (DoS) condition. Continued receipt and processing of this TCP segment could create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS Evolved: 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO; 22.1 versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO.	7.5	More Details
CVE-2022-39058	RAVA certification validation system has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and access arbitrary system files.	7.5	More Details
CVE-2022-41547	Mobile Security Framework (MobSF) v0.9.2 and below was discovered to contain a local file inclusion (LFI) vulnerability in the StaticAnalyzer/views.py script. This vulnerability allows attackers to read arbitrary files via a crafted HTTP request.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42080	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 was discovered to contain a heap overflow via sched_start_time parameter.	7.5	More Details
CVE-2022-42079	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 was discovered to contain a stack overflow via the function formWifiBasicSet.	7.5	More Details
CVE-2022-3283	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions before before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1 While cloning an issue with special crafted content added to the description could have been used to trigger high CPU usage.	7.5	More Details
CVE-2022-23769	Remote code execution vulnerability due to insufficient user privilege verification in reverseWall-MDS. Remote attackers can exploit the vulnerability such as stealing account, through remote code execution.	7.5	More Details
CVE-2021-36369	An issue was discovered in Dropbear through 2020.81. Due to a non-RFC-compliant check of the available authentication methods in the client-side SSH code, it is possible for an SSH server to change the login process in its favor. This attack can bypass additional security measures such as FIDO2 tokens or SSH-Askpass. Thus, it allows an attacker to abuse a forwarded agent for logging on to another server unnoticed.	7.5	More Details
CVE-2022-39278	Istio is an open platform-independent service mesh that provides traffic management, policy enforcement, and telemetry collection. Prior to versions 1.15.2, 1.14.5, and 1.13.9, the Istio control plane, istiod, is vulnerable to a request processing error, allowing a malicious attacker that sends a specially crafted or oversized message which results in the control plane crashing when the Kubernetes validating or mutating webhook service is exposed publicly. This endpoint is served over TLS port 15017, but does not require any authentication from the attacker. For simple installations, Istiod is typically only reachable from within the cluster, limiting the blast radius. However, for some deployments, especially external istiod topologies, this port is exposed over the public internet. Versions 1.15.2, 1.14.5, and 1.13.9 contain patches for this issue. There are no effective workarounds, beyond upgrading. This bug is due to an error in `regexp.Compile` in Go.	7.5	More Details
CVE-2022-39412	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Admin Console). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Access Manager accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2022-2931	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. Malformed content added to the issue description could have been used to trigger high CPU usage.	7.5	More Details
CVE-2022-22201	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2.	7.5	More Details
CVE-2022-29055	A access of uninitialized pointer in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x, FortiProxy version 7.0.0 through 7.0.4, 2.0.0 through 2.0.9, 1.2.x allows a remote unauthenticated or authenticated attacker to crash the sslvpn daemon via an HTTP GET request.	7.5	More Details
CVE-2022-41479	The DevExpress Resource Handler (ASPxHttpHandlerModule) in DevExpress ASP.NET Web Forms Build v19.2.3 does not verify the referenced objects in the /DXR.axd?r= HTTP GET parameter. This leads to an Insecure Direct Object References (IDOR) vulnerability which allows attackers to access the application source code. NOTE: the vendor disputes this because the retrieved source code is only the DevExpress client-side application code that is, of course, intentionally readable by web browsers (a site's custom code and data is never accessible via an IDOR approach).	7.5	More Details
CVE-2022-3382	HIWIN Robot System Software version 3.3.21.9869 does not properly address the terminated command source. As a result, an attacker could craft code to disconnect HRSS and the controller and cause a denial-of-service condition.	7.5	More Details
CVE-2022-3517	A vulnerability was found in the minimatch package. This flaw allows a Regular Expression Denial of Service (ReDoS) when calling the braceExpand function with specific arguments, resulting in a Denial of Service.	7.5	More Details
CVE-2020-8975	ZGR TPS200 NG in its 2.00 firmware version and 1.01 hardware version, allows a remote attacker with access to the web application and knowledge of the routes (URIs) used by the application, to access sensitive information about the system.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22192	An Improper Validation of Syntactic Correctness of Input vulnerability in the kernel of Juniper Networks Junos OS Evolved on PTX series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). When an incoming TCP packet destined to the device is malformed there is a possibility of a kernel panic. Only TCP packets destined to the ports for BGP, LDP and MSDP can trigger this. This issue only affects PTX10004, PTX10008, PTX10016. No other PTX Series devices or other platforms are affected. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S4-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 20.4R1-EVO.	7.5	More Details
CVE-2022-38977	The HwAirlink module has a heap overflow vulnerability.Successful exploitation of this vulnerability may cause out-of-bounds writes, resulting in modification of sensitive data.	7.5	More Details
CVE-2022-39299	Passport-SAML is a SAML 2.0 authentication provider for Passport, the Node.js authentication library. A remote attacker may be able to bypass SAML authentication on a website using passport-saml. A successful attack requires that the attacker is in possession of an arbitrary IDP signed XML element. Depending on the IDP used, fully unauthenticated attacks (e.g without access to a valid user) might also be feasible if generation of a signed message can be triggered. Users should upgrade to passport-saml version 3.2.2 or newer. The issue was also present in the beta releases of `node-saml` before version 4.0.0-beta.5. If you cannot upgrade, disabling SAML authentication may be done as a workaround.	7.4	More Details
CVE-2022-21615	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Data Quality, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N).	7.4	More Details
CVE-2022-3060	Improper control of a resource identifier in Error Tracking in GitLab CE/EE affecting all versions from 12.7 allows an authenticated attacker to generate content which could cause a victim to make unintended arbitrary requests	7.3	More Details
CVE-2022-2865	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions before 15.1.6, 15.2 to 15.2.4 and 15.3 prior to 15.3.2. It was possible to exploit a vulnerability in setting the labels colour feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on behalf of victims at client side.	7.3	More Details
CVE-2022-3368	A vulnerability within the Software Updater functionality of Avira Security for Windows allowed an attacker with write access to the filesystem, to escalate his privileges in certain scenarios. The issue was fixed with Avira Security version 1.1.72.30556.	7.3	More Details
CVE-2022-3465	A vulnerability classified as critical was found in Mediabridge Medialink. This vulnerability affects unknown code of the file /index.asp. The manipulation leads to improper authentication. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-210700.	7.3	More Details
CVE-2022-2527	An issue in Incident Timelines has been discovered in GitLab CE/EE affecting all versions starting from 14.9 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2.which allowed an authenticated attacker to inject arbitrary content. A victim interacting with this content could lead to arbitrary requests.	7.3	More Details
CVE-2022-22248	An Incorrect Permission Assignment vulnerability in shell processing of Juniper Networks Junos OS Evolved allows a low-privileged local user to modify the contents of a configuration file which could cause another user to execute arbitrary commands within the context of the follow-on user's session. If the follow-on user is a high-privileged administrator, the attacker could leverage this vulnerability to take complete control of the target system. While this issue is triggered by a user, other than the attacker, accessing the Junos shell, an attacker simply requires Junos CLI access to exploit this vulnerability. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S1-EVO; All versions of 21.1-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO.	7.3	More Details
CVE-2022-3583	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument business leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-211192.	7.3	More Details
CVE-2022-3495	A vulnerability has been found in SourceCodester Simple Online Public Access Catalog 1.0 and classified as critical. This vulnerability affects unknown code of the file /opac/Actions.php?a=login of the component Admin Login. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-210784.	7.3	More Details
CVE-2022-39421	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28762	Zoom Client for Meetings for macOS (Standard and for IT Admin) starting with 5.10.6 and prior to 5.12.0 contains a debugging port misconfiguration. When camera mode rendering context is enabled as part of the Zoom App Layers API by running certain Zoom Apps, a local debugging port is opened by the Zoom client. A local malicious user could use this debugging port to connect to and control the Zoom Apps running in the Zoom client.	7.3	More Details
CVE-2022-21600	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2022-34022	SQL injection vulnerability in ResIOT IOT Platform + LoRaWAN Network Server through 4.1.1000114 via a crafted POST request to /ResiotQueryDBActive.	7.2	More Details
CVE-2022-41416	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /user/update_booking.php.	7.2	More Details
CVE-2022-41537	Online Tours & Travels Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via the component /user_operations/profile.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-41407	Online Pet Shop We App v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=orders/view_order.	7.2	More Details
CVE-2022-41504	An arbitrary file upload vulnerability in the component /php_action/editProductImage.php of Billing System Project v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-38424	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in arbitrary file system write. Exploitation of this issue does not require user interaction, but does require administrator privileges.	7.2	More Details
CVE-2022-40921	DedeCMS V5.7.99 was discovered to contain an arbitrary file upload vulnerability via the component /dede/file_manage_control.php.	7.2	More Details
CVE-2022-42232	Simple Cold Storage Management System v1.0 is vulnerable to SQL Injection via /csms/classes/Master.php?f=delete_storage.	7.2	More Details
CVE-2022-38421	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, but does require administrator privileges.	7.2	More Details
CVE-2022-41406	An arbitrary file upload vulnerability in the /admin/admin_pic.php component of Church Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-41532	Open Source SACCO Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /sacco_shield/ajax.php?action=delete_plan.	7.2	More Details
CVE-2022-41530	Open Source SACCO Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /sacco_shield/ajax.php?action=delete_borrower.	7.2	More Details
CVE-2022-3552	Unrestricted Upload of File with Dangerous Type in GitHub repository boxbilling/boxbilling prior to 0.0.1.	7.2	More Details
CVE-2022-42142	Online Tours & Travels Management System v1.0 is vulnerable to Arbitrary code execution via ip/tour/admin/operations/update_settings.php.	7.2	More Details
CVE-2022-42143	Open Source SACCO Management System v1.0 is vulnerable to SQL Injection via /sacco_shield/manage_payment.php.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41534	Online Diagnostic Lab Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via the component /php_action/createOrder.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-41536	Open Source SACCO Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /sacco_shield/manage_user.php.	7.2	More Details
CVE-2022-41533	Online Diagnostic Lab Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via the component /php_action/editProductImage.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-41535	Open Source SACCO Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /sacco_shield/manage_borrower.php.	7.2	More Details
CVE-2022-3131	The Search Logger WordPress plugin through 0.9 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users	7.2	More Details
CVE-2022-41498	Billing System Project v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /phpinventory/editbrand.php.	7.2	More Details
CVE-2022-3150	The WP Custom Cursors WordPress plugin before 3.2 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privileged users such as admin	7.2	More Details
CVE-2022-21603	Vulnerability in the Oracle Database - Sharding component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows high privileged attacker having Local Logon privilege with network access via Local Logon to compromise Oracle Database - Sharding. Successful attacks of this vulnerability can result in takeover of Oracle Database - Sharding. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2022-3243	The Import all XML, CSV & TXT WordPress plugin before 6.5.8 does not properly sanitise and escape imported data before using them back SQL statements, leading to SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-21596	Vulnerability in the Oracle Database - Advanced Queuing component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows high privileged attacker having DBA user privilege with network access via Oracle Net to compromise Oracle Database - Advanced Queuing. Successful attacks of this vulnerability can result in takeover of Oracle Database - Advanced Queuing. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2022-39057	RAVA certificate validation system has insufficient filtering for special parameter of the web page input field. A remote attacker with administrator privilege can exploit this vulnerability to perform arbitrary system command and disrupt service.	7.2	More Details
CVE-2022-42218	Open Source SACCO Management System v1.0 vulnerable to SQL Injection via /sacco_shield/manage_loan.php.	7.2	More Details
CVE-2022-41577	The kernel server has a vulnerability of not verifying the length of the data transferred in the user space.Successful exploitation of this vulnerability may cause out-of-bounds read in the kernel, which affects the device confidentiality and availability.	7.1	More Details
CVE-2022-33937	Dell GeoDrive, Versions 1.0 - 2.2, contain a Path Traversal Vulnerability in the reporting function. A local, low privileged attacker could potentially exploit this vulnerability, to gain unauthorized delete access to the files stored on the server filesystem, with the privileges of the GeoDrive service: NT AUTHORITY\SYSTEM.	7.1	More Details
CVE-2022-21593	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: OHS Config MBeans). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HTTP Server accessible data as well as unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).	7.1	More Details
CVE-2022-33922	Dell GeoDrive, versions prior to 2.2, contains Insecure File and Folder Permissions vulnerabilities. A low privilege attacker could potentially exploit this vulnerability, leading to the execution of arbitrary code in the SYSTEM security context. Dell recommends customers to upgrade at the earliest opportunity.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33921	Dell GeoDrive, versions prior to 2.2, contains Multiple DLL Hijacking Vulnerabilities. A low privilege attacker could potentially exploit this vulnerability, leading to the execution of arbitrary code in the SYSTEM security context.	7.0	More Details
CVE-2022-31037	OroCommerce is an open-source Business to Business Commerce application. Versions between 4.1.0 and 4.1.17 inclusive, 4.2.0 and 4.2.11 inclusive, and between 5.0.0 and 5.0.3 inclusive, are vulnerable to Cross-site Scripting in the UPS Surcharge field of the Shipping rule edit page. The attacker needs permission to create or edit a shipping rule. This issue has been patched in version 5.0.6. There are no known workarounds.	6.9	More Details
CVE-2022-33873	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in Console login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated attacker to execute arbitrary command in the underlying shell.	6.8	More Details
CVE-2022-39201	Grafana is an open source observability and data visualization platform. Starting with version 5.0.0-beta1 and prior to versions 8.5.14 and 9.1.8, Grafana could leak the authentication cookie of users to plugins. The vulnerability impacts data source and plugin proxy endpoints under certain conditions. The destination plugin could receive a user's Grafana authentication cookie. Versions 9.1.8 and 8.5.14 contain a patch for this issue. There are no known workarounds.	6.8	More Details
CVE-2022-42464	OpenHarmony-v3.1.2 and prior versions, 3.0.6 and prior versions have a Kernel memory pool override vulnerability in /dev/mmz_userdev device driver. The impact depends on the privileges of the attacker. The unprivileged process run on the device could disclose sensitive information including kernel pointer, which could be used in further attacks. The processes with system user UID run on the device would be able to mmap memory pools used by kernel and override them which could be used to gain kernel code execution on the device, gain root privileges, or cause device reboot.	6.7	More Details
CVE-2022-35844	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the management interface of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to commands of the certificate import feature.	6.7	More Details
CVE-2022-35041	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b558f.	6.5	More Details
CVE-2022-41606	HashiCorp Nomad and Nomad Enterprise 1.0.2 up to 1.2.12, and 1.3.5 jobs submitted with an artifact stanza using invalid S3 or GCS URLs can be used to crash client agents. Fixed in 1.2.13, 1.3.6, and 1.4.0.	6.5	More Details
CVE-2022-28291	Insufficiently Protected Credentials: An authenticated user with debug privileges can retrieve stored Nessus policy credentials from the “nessusd” process in cleartext via process dumping. The affected products are all versions of Nessus Essentials and Professional. The vulnerability allows an attacker to access credentials stored in Nessus scanners, potentially compromising its customers’ network of assets.	6.5	More Details
CVE-2022-35047	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b05aa.	6.5	More Details
CVE-2022-3082	The miniOrange Discord Integration WordPress plugin before 2.1.6 does not have authorisation and CSRF in some of its AJAX actions, allowing any logged in users, such as subscriber to call them, and disable the app for example	6.5	More Details
CVE-2022-35046	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b0466.	6.5	More Details
CVE-2022-35045	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b0d63.	6.5	More Details
CVE-2022-21601	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.4.0-12.0.0.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Billing and Revenue Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	6.5	More Details
CVE-2022-2455	A business logic issue in the handling of large repositories in all versions of GitLab CE/EE from 10.0 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2 allowed an authenticated and authorized user to exhaust server resources by importing a malicious project.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2533	An issue has been discovered in GitLab affecting all versions starting from 12.10 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. GitLab was not performing correct authentication with some Package Registries when IP address restrictions were configured, allowing an attacker already in possession of a valid Deploy Token to misuse it from any location.	6.5	More Details
CVE-2022-2592	A lack of length validation in Snippet descriptions in GitLab CE/EE affecting all versions prior to 15.1.6, 15.2 prior to 15.2.4 and 15.3 prior to 15.3.2 allows an authenticated attacker to create a maliciously large Snippet which when requested with or without authentication places excessive load on the server, potential leading to Denial of Service.	6.5	More Details
CVE-2022-39308	GoCD is a continuous delivery server. GoCD helps you automate and streamline the build-test-release cycle for continuous delivery of your product. GoCD versions from 19.2.0 to 19.10.0 (inclusive) are subject to a timing attack in validation of access tokens due to use of regular string comparison for validation of the token rather than a constant time algorithm. This could allow a brute force attack on GoCD server API calls to observe timing differences in validations in order to guess an access token generated by a user for API access. This issue is fixed in GoCD version 19.11.0. As a workaround, users can apply rate limiting or insert random delays to API calls made to GoCD Server via a reverse proxy or other fronting web server. Another workaround, users may disallow use of access tokens by users by having an administrator revoke all access tokens through the "Access Token Management" admin function.	6.5	More Details
CVE-2022-42077	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolReboot.	6.5	More Details
CVE-2022-3540	An issue has been discovered in hunter2 affecting all versions before 2.1.0. Improper handling of auto-completion input allows an authenticated attacker to extract other users email addresses	6.5	More Details
CVE-2022-35044	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x617087.	6.5	More Details
CVE-2022-41471	74cmsSE v3.12.0 allows authenticated attackers with low-level privileges to arbitrarily change the rights and credentials of the Super Administrator account.	6.5	More Details
CVE-2022-35136	Boodskap IoT Platform v4.4.9-02 allows attackers to make unauthenticated API requests.	6.5	More Details
CVE-2022-35043	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6c08a6.	6.5	More Details
CVE-2022-3067	An issue has been discovered in the Import functionality of GitLab CE/EE affecting all versions starting from 14.4 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. It was possible for an authenticated user to read arbitrary projects' content given the project's ID.	6.5	More Details
CVE-2022-39408	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2022-3165	An integer underflow issue was found in the QEMU VNC server while processing ClientCutText messages in the extended format. A malicious client could use this flaw to make QEMU unresponsive by sending a specially crafted payload message, resulting in a denial of service.	6.5	More Details
CVE-2022-3291	Serialization of sensitive data in GitLab EE affecting all versions from 14.9 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 can leak sensitive information via cache	6.5	More Details
CVE-2022-35042	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x4adb11.	6.5	More Details
CVE-2022-35040	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b5567.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39410	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2022-42087	Tenda AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolReboot.	6.5	More Details
CVE-2022-35056	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b0478.	6.5	More Details
CVE-2022-41474	RPCMS v3.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily change the password of any account.	6.5	More Details
CVE-2022-42086	Tenda AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4 is vulnerable to Cross Site Request Forgery (CSRF) via function TendaAteMode.	6.5	More Details
CVE-2022-35059	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6c0414.	6.5	More Details
CVE-2022-22230	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2.	6.5	More Details
CVE-2022-35050	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b04de.	6.5	More Details
CVE-2022-2850	A flaw was found In 389-ds-base. When the Content Synchronization plugin is enabled, an authenticated user can reach a NULL pointer dereference using a specially crafted query. This flaw allows an authenticated attacker to cause a denial of service. This CVE is assigned against an incomplete fix of CVE-2021-3514.	6.5	More Details
CVE-2022-35051	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b55af.	6.5	More Details
CVE-2022-35049	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b03b5.	6.5	More Details
CVE-2022-21635	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).	6.5	More Details
CVE-2022-35048	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b0b2c.	6.5	More Details
CVE-2022-21636	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Session Management). Supported versions that are affected are 12.2.6-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2828	In affected versions of Octopus Server it is possible to reveal information about teams via the API due to an Insecure Direct Object Reference (IDOR) vulnerability	6.5	More Details
CVE-2022-35052	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b84b1.	6.5	More Details
CVE-2022-39065	A single malformed IEEE 802.15.4 (Zigbee) frame makes the TRÅDFRI gateway unresponsive, such that connected lighting cannot be controlled with the IKEA Home Smart app and TRÅDFRI remote control. The malformed Zigbee frame is an unauthenticated broadcast message, which means all vulnerable devices within radio range are affected. CVSS 3.1 Base Score: 6.5 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.5	More Details
CVE-2022-35058	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b05ce.	6.5	More Details
CVE-2022-22250	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.	6.5	More Details
CVE-2022-28760	Zoom On-Premise Meeting Connector MMR before version 4.8.20220815.130 contains an improper access control vulnerability. As a result, a malicious actor could obtain the audio and video feed of a meeting they were not authorized to join and cause other meeting disruptions.	6.5	More Details
CVE-2022-22226	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1.	6.5	More Details
CVE-2022-28761	Zoom On-Premise Meeting Connector MMR before version 4.8.20220916.131 contains an improper access control vulnerability. As a result, a malicious actor in a meeting or webinar they are authorized to join could prevent participants from receiving audio and video causing meeting disruptions.	6.5	More Details
CVE-2022-35053	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x61731f.	6.5	More Details
CVE-2022-22224	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22223	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 l refresh 1 l no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 l no-more l match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE	6.5	More Details
CVE-2022-35054	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6171b2.	6.5	More Details
CVE-2022-35055	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6c0473.	6.5	More Details
CVE-2022-22237	An Improper Authentication vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause an impact on confidentiality or integrity. A vulnerability in the processing of TCP-AO will allow a BGP or LDP peer not configured with authentication to establish a session even if the peer is locally configured to use authentication. This could lead to untrusted or unauthorized sessions being established. This issue affects Juniper Networks Junos OS: 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS Evolved.	6.5	More Details
CVE-2022-22249	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071): EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071): EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071): EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2.	6.5	More Details
CVE-2022-42078	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolRestoreSet.	6.5	More Details
CVE-2022-2428	A crafted tag in the Jupyter Notebook viewer in GitLab EE/CE affecting all versions before 15.1.6, 15.2 to 15.2.4, and 15.3 to 15.3.2 allows an attacker to issue arbitrary HTTP requests	6.4	More Details
CVE-2022-3492	A vulnerability classified as critical was found in SourceCodester Human Resource Management System 1.0. This vulnerability affects unknown code of the component Profile Photo Handler. The manipulation of the argument parameter leads to os command injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB-210772.	6.3	More Details
CVE-2022-3471	A vulnerability was found in SourceCodester Human Resource Management System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file city.php. The manipulation of the argument searccity leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-210715.	6.3	More Details
CVE-2022-3472	A vulnerability was found in SourceCodester Human Resource Management System. It has been rated as critical. Affected by this issue is some unknown functionality of the file city.php. The manipulation of the argument cityedit leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-210716.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3504	A vulnerability was found in SourceCodester Sanitization Management System and classified as critical. This issue affects some unknown processing of the file /php-sms/?p=services/view_service. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-210839.	6.3	More Details
CVE-2022-3496	A vulnerability was found in SourceCodester Human Resource Management System 1.0 and classified as critical. This issue affects some unknown processing of the file employeeadd.php of the component Admin Panel. The manipulation leads to improper access controls. The attack may be initiated remotely. The identifier VDB-210785 was assigned to this vulnerability.	6.3	More Details
CVE-2022-3470	A vulnerability was found in SourceCodester Human Resource Management System. It has been classified as critical. Affected is an unknown function of the file getstatecity.php. The manipulation of the argument sc leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-210714 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-3458	A vulnerability has been found in SourceCodester Human Resource Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /employeeview.php of the component Image File Handler. The manipulation leads to unrestricted upload. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-210559.	6.3	More Details
CVE-2022-3473	A vulnerability classified as critical has been found in SourceCodester Human Resource Management System. This affects an unknown part of the file getstatecity.php. The manipulation of the argument ci leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-210717 was assigned to this vulnerability.	6.3	More Details
CVE-2022-3579	A vulnerability classified as critical was found in SourceCodester Cashier Queuing System 1.0. This vulnerability affects unknown code of the file /queuing/login.php of the component Login Page. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-211186 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-3584	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file edituser.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-211193 was assigned to this vulnerability.	6.3	More Details
CVE-2022-35944	October is a self-hosted Content Management System (CMS) platform based on the Laravel PHP Framework. This vulnerability only affects installations that rely on the safe mode restriction, commonly used when providing public access to the admin panel. Assuming an attacker has access to the admin panel and permission to open the "Editor" section, they can bypass the Safe Mode (`cms.safe_mode`) restriction to introduce new PHP code in a CMS template using a specially crafted request. The issue has been patched in versions 2.2.34 and 3.0.66.	6.2	More Details
CVE-2021-22685	An attacker may be able to use minify route with a relative path to view any file on the Cassia Networks Access Controller prior to 2.0.1.	6.2	More Details
CVE-2022-21631	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Design Tools SEC). Supported versions that are affected are 9.2.6.4 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-21639	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search Integration). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-42117	A Cross-site scripting (XSS) vulnerability in the Frontend Taglib module in Liferay Portal 7.3.2 through 7.4.3.16, and Liferay DXP 7.3 before update 6, and 7.4 before update 17 allows remote attackers to inject arbitrary web script or HTML.	6.1	More Details
CVE-2022-41351	In Zimbra Collaboration Suite (ZCS) 8.8.15, at the URL /h/calendar, one can trigger XSS by adding JavaScript code to the view parameter and changing the value of the uncheck parameter to a string (instead of default value of 10).	6.1	More Details
CVE-2022-3149	The WP Custom Cursors WordPress plugin before 3.0.1 does not have CSRF check in place when creating and editing cursors, which could allow attackers to made a logged in admin perform such actions via CSRF attacks. Furthermore, due to the lack of sanitisation and escaping in some of the cursor options, it could also lead to Stored Cross-Site Scripting	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21606	Vulnerability in the Oracle Services for Microsoft Transaction Server component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Services for Microsoft Transaction Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Services for Microsoft Transaction Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Services for Microsoft Transaction Server accessible data as well as unauthorized read access to a subset of Oracle Services for Microsoft Transaction Server accessible data. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-42071	Online Birth Certificate Management System version 1.0 suffers from a Cross Site Scripting (XSS) Vulnerability.	6.1	More Details
CVE-2022-42066	Online Examination System version 1.0 suffers from a cross site scripting vulnerability via index.php.	6.1	More Details
CVE-2022-39295	Knowage is an open source suite for modern business analytics alternative over big data systems. KnowageLabs / Knowage-Server starting with the 6.x branch and prior to versions 7.4.22, 8.0.9, and 8.1.0 is vulnerable to cross-site scripting because the `XSSRequestWrapper::stripXSS` method can be bypassed. Versions 7.4.22, 8.0.9, and 8.1.0 contain patches for this issue. There are no known workarounds.	6.1	More Details
CVE-2022-42715	A reflected XSS vulnerability exists in REDCap before 12.04.18 in the Alerts & Notifications upload feature. A crafted CSV file will, when uploaded, trigger arbitrary JavaScript code execution.	6.1	More Details
CVE-2022-21630	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are 9.2.6.4 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2022-40605	MITRE CALDERA before 4.1.0 allows XSS in the Operations tab and/or Debrief plugin via a crafted operation name, a different vulnerability than CVE-2022-40606.	6.1	More Details
CVE-2022-22242	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2.	6.1	More Details
CVE-2022-42113	A Cross-site scripting (XSS) vulnerability in Document Library module in Liferay Portal 7.4.3.30 through 7.4.3.36, and Liferay DXP 7.4 update 30 through update 36 allows remote attackers to inject arbitrary web script or HTML via the `redirect` parameter.	6.1	More Details
CVE-2022-41349	In Zimbra Collaboration Suite (ZCS) 8.8.15, the URL at /h/compose accepts an attachUrl parameter that is vulnerable to Reflected XSS. This allows executing arbitrary JavaScript on the victim's machine.	6.1	More Details
CVE-2022-42147	kkFileView 4.0 is vulnerable to Cross Site Scripting (XSS) via controller\ Filecontroller.java.	6.1	More Details
CVE-2022-40606	MITRE CALDERA before 4.1.0 allows XSS in the Operations tab and/or Debrief plugin via a crafted operation name, a different vulnerability than CVE-2022-40605.	6.1	More Details
CVE-2022-40440	mxGraph v4.2.2 was discovered to contain a cross-site scripting (XSS) vulnerability via the setTooltips() function.	6.1	More Details
CVE-2022-41473	RPCMS v3.0.2 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in the Search function.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42202	TP-Link TL-WR841N 8.0 4.17.16 Build 120201 Rel.54750n is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2022-31123	Grafana is an open source observability and data visualization platform. Versions prior to 9.1.8 and 8.5.14 are vulnerable to a bypass in the plugin signature verification. An attacker can convince a server admin to download and successfully run a malicious plugin even though unsigned plugins are not allowed. Versions 9.1.8 and 8.5.14 contain a patch for this issue. As a workaround, do not install plugins downloaded from untrusted sources.	6.1	More Details
CVE-2022-41348	An issue was discovered in Zimbra Collaboration (ZCS) 9.0. XSS can occur via the onerror attribute of an IMG element, leading to information disclosure.	6.1	More Details
CVE-2022-41350	In Zimbra Collaboration Suite (ZCS) 8.8.15, /h/search?action=voicemail&action=listen accepts a phone parameter that is vulnerable to Reflected XSS. This allows executing arbitrary JavaScript on the victim's machine.	6.1	More Details
CVE-2022-42116	A Cross-site scripting (XSS) vulnerability in the Frontend Editor module's integration with CKEditor in Liferay Portal 7.3.2 through 7.4.3.14, and Liferay DXP 7.3 before update 6, and 7.4 before update 15 allows remote attackers to inject arbitrary web script or HTML via the (1) name, or (2) namespace parameter.	6.1	More Details
CVE-2022-32493	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	6.0	More Details
CVE-2022-36439	AsusSoftwareManager.exe in ASUS System Control Interface on ASUS personal computers (running Windows) allows a local user to write into the Temp directory and delete another more privileged file via SYSTEM privileges. This affects ASUS System Control Interface 3 before 3.1.5.0, AsusSoftwareManger.exe before 1.0.53.0, and AsusLiveUpdate.dll before 1.0.45.0.	6.0	More Details
CVE-2022-39423	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.38. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2022-21621	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	6.0	More Details
CVE-2022-22235	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1.	5.9	More Details
CVE-2022-3206	The Passster WordPress plugin before 3.5.5.5.2 stores the password inside a cookie named "passster" using base64 encoding method which is easy to decode. This puts the password at risk in case the cookies get leaked.	5.9	More Details
CVE-2022-22225	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22220	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1.	5.9	More Details
CVE-2022-22219	Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved, an attacker in direct control of a BGP client connected to a route reflector, or via a machine in the middle (MITM) attack, can send a specific EVPN route contained within a BGP Update, triggering a routing protocol daemon (RPD) crash, leading to a Denial of Service (DoS) condition. Continued receipt and processing of these specific EVPN routes could create a sustained Denial of Service (DoS) condition. This issue only occurs on BGP route reflectors, only within a BGP EVPN multicast environment, and only when one or more BGP clients have 'leave-sync-route-oldstyle' enabled. This issue affects: Juniper Networks Junos OS 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R3; 22.2 versions prior to 22.2R2. Juniper Networks Junos OS Evolved 21.3 version 21.3R1-EVO and later versions prior to 21.4R3-EVO; 22.1 versions prior to 22.1R1-S2-EVO, 22.1R3-EVO; 22.2 versions prior to 22.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.3R1. Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO.	5.9	More Details
CVE-2022-22208	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO.	5.9	More Details
CVE-2022-41540	The web app client of TP-Link AX10v1 V1_211117 uses hard-coded cryptographic keys when communicating with the router. Attackers who are able to intercept the communications between the web client and router through a man-in-the-middle attack can then obtain the sequence key via a brute-force attack, and access sensitive information.	5.9	More Details
CVE-2022-39283	FreeRDP is a free remote desktop protocol library and clients. All FreeRDP based clients when using the `/video` command line switch might read uninitialized data, decode it as audio/video and display the result. FreeRDP based server implementations are not affected. This issue has been patched in version 2.8.1. If you cannot upgrade do not use the `/video` switch.	5.9	More Details
CVE-2022-21609	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Server). The supported version that is affected is 5.9.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N).	5.7	More Details
CVE-2022-3421	An attacker can pre-create the `/Applications/Google\ Drive.app/Contents/MacOS` directory which is expected to be owned by root to be owned by a non-root user. When the Drive for Desktop installer is run for the first time, it will place a binary in that directory with execute permissions and set its setuid bit. Since the attacker owns the directory, the attacker can replace the binary with a symlink, causing the installer to set the setuid bit on the symlink. When the symlink is executed, it will run with root permissions. We recommend upgrading past version 64.0	5.6	More Details
CVE-2022-32483	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	5.6	More Details
CVE-2022-32484	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	5.6	More Details
CVE-2022-39125	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-38449	Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38688	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2022-38437	Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-38687	In messaging service, there is a missing permission check. This could lead to local denial of service in messaging service with no additional execution privileges needed.	5.5	More Details
CVE-2022-38443	Adobe Dimension versions 3.4.5 is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-38679	In music service, there is a missing permission check. This could lead to local denial of service in music service with no additional execution privileges needed.	5.5	More Details
CVE-2022-38677	In cell service, there is a missing permission check. This could lead to local denial of service in cell service with no additional execution privileges needed.	5.5	More Details
CVE-2022-38676	In gpu driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-2984	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-38673	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39417	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2022-38672	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39401	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2022-39117	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2022-42342	Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-38689	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2022-38690	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-35691	Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39113	In Music service, there is a missing permission check. This could lead to local denial of service in Music service with no additional execution privileges needed.	5.5	More Details
CVE-2022-39121	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39122	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39123	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39124	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39115	In Music service, there is a missing permission check. This could lead to local denial of service in Music service with no additional execution privileges needed.	5.5	More Details
CVE-2022-39114	In Music service, there is a missing permission check. This could lead to local denial of service in Music service with no additional execution privileges needed.	5.5	More Details
CVE-2022-3564	A vulnerability classified as critical was found in Linux Kernel. Affected by this vulnerability is the function l2cap_reassemble_sdu of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211087.	5.5	More Details
CVE-2022-38697	In messaging service, there is a missing permission check. This could lead to access unexpected provider in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-39112	In Music service, there is a missing permission check. This could lead to local denial of service in Music service with no additional execution privileges needed.	5.5	More Details
CVE-2022-39126	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39127	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39105	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39103	In Gallery service, there is a missing permission check. This could lead to local denial of service in Gallery service with no additional execution privileges needed.	5.5	More Details
CVE-2022-39128	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-38671	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39120	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-35080	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via png_load at /lib/png.c.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20464	In various functions of ap_input_processor.c, there is a possible way to record audio during a phone call due to a logic error in the code. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-236042696References: N/A	5.5	More Details
CVE-2022-3534	A vulnerability classified as critical has been found in Linux Kernel. Affected is the function btf_dump_name_dups of the file tools/lib/bpf/btf_dump.c of the component libbpf. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211032.	5.5	More Details
CVE-2022-39407	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	5.5	More Details
CVE-2022-3541	A vulnerability classified as critical has been found in Linux Kernel. This affects the function spl2sw_nvmem_get_mac_address of the file drivers/net/ethernet/sunplus/spl2sw_driver.c of the component BPF. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier VDB-211041 was assigned to this vulnerability.	5.5	More Details
CVE-2022-3467	A vulnerability classified as critical was found in Jiusi OA. Affected by this vulnerability is an unknown functionality of the file /jsoa/hntdCustomDesktopActionContent. The manipulation of the argument inforid leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-210709 was assigned to this vulnerability.	5.5	More Details
CVE-2022-3545	A vulnerability has been found in Linux Kernel and classified as critical. Affected by this vulnerability is the function area_cache_get of the file drivers/net/ethernet/netronome/nfp/nfpcore/nfp_cppcore.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier VDB-211045 was assigned to this vulnerability.	5.5	More Details
CVE-2022-35081	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via png_read_header at /src/png2swf.c.	5.5	More Details
CVE-2022-22240	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1.	5.5	More Details
CVE-2022-42722	In the Linux kernel 5.8 through 5.19.x before 5.19.16, local attackers able to inject WLAN frames into the mac80211 stack could cause a NULL pointer dereference denial-of-service attack against the beacon protection of P2P devices.	5.5	More Details
CVE-2022-3550	A vulnerability classified as critical was found in X.org Server. Affected by this vulnerability is the function _GetCountedString of the file xkb/xkb.c. The manipulation leads to buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211051.	5.5	More Details
CVE-2022-22234	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2.	5.5	More Details
CVE-2022-42721	A list management bug in BSS handling in the mac80211 stack in the Linux kernel 5.1 through 5.19.x before 5.19.16 could be used by local attackers (able to inject WLAN frames) to corrupt a linked list and, in turn, potentially execute code.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33918	Dell GeoDrive, Versions 2.1 - 2.2, contains an information disclosure vulnerability. An authenticated non-admin user could potentially exploit this vulnerability and gain access to sensitive information.	5.5	More Details
CVE-2022-39302	Ree6 is a moderation bot. This vulnerability would allow other server owners to create configurations such as "Better-Audit-Logging" which contain a channel from another server as a target. This would mean you could send log messages to another Guild channel and bypass raid and webhook protections. A specifically crafted log message could allow spamming and mass advertisements. This issue has been patched in version 1.9.9. There are currently no known workarounds.	5.5	More Details
CVE-2022-22233	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). In Segment Routing (SR) to Label Distribution Protocol (LDP) interworking scenario, configured with Segment Routing Mapping Server (SRMS) at any node, when an Area Border Router (ABR) leaks the SRMS entries having "S" flag set from IS-IS Level 2 to Level 1, an rpd core might be observed when a specific low privileged CLI command is issued. This issue affects: Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R2. Juniper Networks Junos OS Evolved 21.4-EVO versions prior to 21.4R1-S2-EVO, 21.4R2-S1-EVO, 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.4R1. Juniper Networks Junos OS Evolved versions prior to 21.4R1-EVO.	5.5	More Details
CVE-2022-42115	Cross-site scripting (XSS) vulnerability in the Object module's edit object details page in Liferay Portal 7.4.3.4 through 7.4.3.36 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into the object field's `Label` text field.	5.4	More Details
CVE-2022-42069	Online Birth Certificate Management System version 1.0 suffers from a persistent Cross Site Scripting (XSS) vulnerability.	5.4	More Details
CVE-2022-41139	MITRE CALDERA 4.1.0 allows stored XSS via app.contact.gist (aka the gist contact configuration field), leading to execution of arbitrary commands on agents.	5.4	More Details
CVE-2022-3339	A reflected cross-site scripting (XSS) vulnerability in ePO prior to 5.10 Update 14 allows a remote unauthenticated attacker to potentially obtain access to an ePO administrator's session by convincing the authenticated ePO administrator to click on a carefully crafted link. This would lead to limited access to sensitive information and limited ability to alter some information in ePO.	5.4	More Details
CVE-2022-38902	A Cross-site scripting (XSS) vulnerability in the Blog module - add new topic functionality in Liferay Digital Experience Platform 7.3.10 SP3 allows remote attackers to inject arbitrary JS script or HTML into the name field of newly created topic.	5.4	More Details
CVE-2022-3338	An External XML entity (XXE) vulnerability in ePO prior to 5.10 Update 14 can lead to an unauthenticated remote attacker to potentially trigger a Server Side Request Forgery attack. This can be exploited by mimicking the Agent Handler call to ePO and passing the carefully constructed XML file through the API.	5.4	More Details
CVE-2022-3506	Cross-site Scripting (XSS) - Stored in GitHub repository barrykooij/related-posts-for-wp prior to 2.1.3.	5.4	More Details
CVE-2022-41431	xzs v3.8.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /admin/question/edit. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title text field.	5.4	More Details
CVE-2022-35612	A cross-site scripting (XSS) vulnerability in MQTTRoute v3.3 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the dashboard name text field.	5.4	More Details
CVE-2022-21629	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are 9.2.6.4 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2022-3066	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. It was possible for an unauthorised user to create issues in a project.	5.4	More Details
CVE-2022-41472	74cmsSE v3.12.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /apiadmin/notice/add. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21591	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: UI Infrastructure). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Transportation Management. CVSS 3.1 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).	5.4	More Details
CVE-2022-42114	A Cross-site scripting (XSS) vulnerability in the Role module's edit role assignees page in Liferay Portal 7.4.0 through 7.4.3.36, and Liferay DXP 7.4 before update 37 allows remote attackers to inject arbitrary web script or HTML.	5.4	More Details
CVE-2022-34021	Multiple Cross Site Scripting (XSS) vulnerabilities in ResIOT IOT Platform + LoRaWAN Network Server through 4.1.1000114 via the form fields.	5.4	More Details
CVE-2022-39420	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Data, Functional Security). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2022-35134	Boodskap IoT Platform v4.4.9-02 contains a cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2022-41542	devhub 0.102.0 was discovered to contain a broken session control.	5.4	More Details
CVE-2022-42112	A Cross-site scripting (XSS) vulnerability in the Portal Search module's Sort widget in Liferay Portal 7.2.0 through 7.4.3.24, and Liferay DXP 7.2 before fix pack 19, 7.3 before update 5, and DXP 7.4 before update 25 allows remote attackers to inject arbitrary web script or HTML via a crafted payload.	5.4	More Details
CVE-2022-22244	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2.	5.3	More Details
CVE-2022-21628	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details
CVE-2022-41587	Uncaptured exceptions in the home screen module. Successful exploitation of this vulnerability may affect stability.	5.3	More Details
CVE-2022-39055	RAVA certificate validation system has inadequate filtering for URL parameter. An unauthenticated remote attacker can perform SSRF attack to discover internal network topology base on query response.	5.3	More Details
CVE-2022-21626	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22238	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO.	5.3	More Details
CVE-2022-22227	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated network-based attacker to cause a partial Denial of Service (DoS). On receipt of specific IPv6 transit traffic, Junos OS Evolved on ACX7100-48L, ACX7100-32C and ACX7509 sends this traffic to the Routing Engine (RE) instead of forwarding it, leading to increased CPU utilization of the RE and a partial DoS. This issue only affects systems configured with IPv6. This issue does not affect ACX7024 which is supported from 22.3R1-EVO onwards where the fix has already been incorporated as indicated in the solution section. This issue affects Juniper Networks Junos OS Evolved on ACX7100-48L, ACX7100-32C, ACX7509: 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S2-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO.	5.3	More Details
CVE-2022-2834	The Helpful WordPress plugin before 4.5.26 puts the exported logs and feedbacks in a publicly accessible location and guessable names, which could allow attackers to download them and retrieve sensitive information such as IP, Names and Email Address depending on the plugin's settings	5.3	More Details
CVE-2022-3526	A vulnerability classified as problematic was found in Linux Kernel. This vulnerability affects the function macvlan_handle_frame of the file drivers/net/macvlan.c of the component skb. The manipulation leads to memory leak. The attack can be initiated remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211024.	5.3	More Details
CVE-2022-21618	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JGSS). Supported versions that are affected are Oracle Java SE: 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details
CVE-2022-21597	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaScript). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2022-3594	A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function intr_callback of the file drivers/net/usb/r8152.c of the component BPF. The manipulation leads to logging of excessive data. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211363.	5.3	More Details
CVE-2022-2720	In affected versions of Octopus Server it was identified that when a sensitive value is a substring of another value, sensitive value masking will only partially work.	5.3	More Details
CVE-2022-3523	A vulnerability was found in Linux Kernel. It has been classified as problematic. Affected is an unknown function of the file mm/memory.c of the component Driver Handler. The manipulation leads to use after free. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211020.	5.3	More Details
CVE-2022-42969	The py library through 1.11.0 for Python allows remote attackers to conduct a ReDoS (Regular expression Denial of Service) attack via a Subversion repository with crafted info data, because the InfoSvnCommand argument is mishandled. Note: This has been disputed by multiple third parties as not being reproduceable and they argue this is not a valid vulnerability.	5.3	More Details
CVE-2022-39405	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Access Manager accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details
CVE-2022-42961	An issue was discovered in wolfSSL before 5.5.0. A fault injection attack on RAM via Rowhammer leads to ECDSA key disclosure. Users performing signing operations with private ECC keys, such as in server-side TLS connections, might leak faulty ECC signatures. These signatures can be processed via an advanced technique for ECDSA key recovery. (In 5.5.0 and later, WOLFSSL_CHECK_SIG_FAULTS can be used to address the vulnerability.)	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41316	HashiCorp Vault and Vault Enterprise's TLS certificate auth method did not initially load the optionally configured CRL issued by the role's CA into memory on startup, resulting in the revocation list not being checked if the CRL has not yet been retrieved. Fixed in 1.12.0, 1.11.4, 1.10.7, and 1.9.10.	5.3	More Details
CVE-2022-3286	Lack of IP address checking in GitLab EE affecting all versions from 14.2 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows a group member to bypass IP restrictions when using a deploy token	5.3	More Details
CVE-2022-21602	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2020-15853	supybot-fedora implements the command 'refresh', that refreshes the cache of all users from FAS. This takes quite a while to run, and zodbot stops responding to requests during this time.	5.3	More Details
CVE-2022-35689	Adobe Commerce versions 2.4.4-p1 (and earlier) and 2.4.5 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to impact the availability of a user's minor feature. Exploitation of this issue does not require user interaction.	5.3	More Details
CVE-2022-21616	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle WebLogic Server executes to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:H).	5.2	More Details
CVE-2022-41686	OpenHarmony-v3.1.2 and prior versions, 3.0.6 and prior versions have an Out-of-bound memory read and write vulnerability in /dev/mmz_userdev device driver. The impact depends on the privileges of the attacker. The unprivileged process run on the device could read out-of-bound memory leading sensitive to information disclosure. The processes with system user UID run on the device would be able to write out-of-bound memory which could lead to unspecified memory corruption.	5.1	More Details
CVE-2022-31130	Grafana is an open source observability and data visualization platform. Versions of Grafana for endpoints prior to 9.1.8 and 8.5.14 could leak authentication tokens to some destination plugins under some conditions. The vulnerability impacts data source and plugin proxy endpoints with authentication tokens. The destination plugin could receive a user's Grafana authentication token. Versions 9.1.8 and 8.5.14 contain a patch for this issue. As a workaround, do not use API keys, JWT authentication, or any HTTP Header based authentication.	4.9	More Details
CVE-2022-21608	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.39 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-21594	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-21641	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-21607	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-21605	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21604	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-38423	Adobe ColdFusion versions Update 14 (and earlier) and Update 4 (and earlier) are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in information disclosure. Exploitation of this issue does not require user interaction, but does require administrator privileges.	4.9	More Details
CVE-2022-36802	The ManageJiraConnectors API in Atlassian Jira Align before version 10.109.2 allows remote attackers to exploit this issue to access internal network resources via a Server-Side Request Forgery. This can be exploited by a remote, unauthenticated attacker with Super Admin privileges by sending a specially crafted HTTP request.	4.9	More Details
CVE-2022-21637	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-21640	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-21599	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-21633	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-21632	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-39411	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Business Process Automation). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Transportation Management accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2022-39310	GoCD is a continuous delivery server. GoCD helps you automate and streamline the build-test-release cycle for continuous delivery of your product. GoCD versions prior to 21.1.0 can allow one authenticated agent to impersonate another agent, and thus receive work packages for other agents due to broken access control and incorrect validation of agent tokens within the GoCD server. Since work packages can contain sensitive information such as credentials intended only for a given job running against a specific agent environment, this can cause accidental information disclosure. Exploitation requires knowledge of agent identifiers and ability to authenticate as an existing agent with the GoCD server. This issue is fixed in GoCD version 21.1.0. There are currently no known workarounds.	4.9	More Details
CVE-2022-39309	GoCD is a continuous delivery server. GoCD helps you automate and streamline the build-test-release cycle for continuous delivery of your product. GoCD versions prior to 21.1.0 leak the symmetric key used to encrypt/decrypt any secure variables/secrets in GoCD configuration to authenticated agents. A malicious/compromised agent may then expose that key from memory, and potentially allow an attacker the ability to decrypt secrets intended for other agents/environments if they also are able to obtain access to encrypted configuration values from the GoCD server. This issue is fixed in GoCD version 21.1.0. There are currently no known workarounds.	4.9	More Details
CVE-2022-39400	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21638	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-21617	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 5.7.39 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2022-2563	The Tutor LMS WordPress plugin before 2.0.10 does not escape some course parameters, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-26375	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mammothology AB Press Optimizer plugin <= 1.1.1 on WordPress.	4.8	More Details
CVE-2022-3139	The We're Open! WordPress plugin before 1.42 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-2574	The Meks Easy Social Share WordPress plugin before 1.2.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-3549	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /csms/admin/?page=user/manage_user of the component Avatar Handler. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-211049 was assigned to this vulnerability.	4.7	More Details
CVE-2022-3566	A vulnerability, which was classified as problematic, was found in Linux Kernel. This affects the function tcp_getsockopt/tcp_setsockopt of the component TCP Handler. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. The identifier VDB-211089 was assigned to this vulnerability.	4.6	More Details
CVE-2022-3565	A vulnerability, which was classified as critical, has been found in Linux Kernel. Affected by this issue is the function del_timer of the file drivers/isdn/mISDN/l1oip_core.c of the component Bluetooth. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211088.	4.6	More Details
CVE-2022-3567	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function inet6_stream_ops/inet6_dgram_ops of the component IPv6 Handler. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. VDB-211090 is the identifier assigned to this vulnerability.	4.6	More Details
CVE-2022-3559	A vulnerability was found in Exim and classified as problematic. This issue affects some unknown processing of the component Regex Handler. The manipulation leads to use after free. The name of the patch is 4e9ed49f8f12eb331b29bd5b6dc3693c520fddc2. It is recommended to apply a patch to fix this issue. The identifier VDB-211073 was assigned to this vulnerability.	4.6	More Details
CVE-2022-21595	Vulnerability in the MySQL Server product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2022-21627	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2022-21625	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2022-3585	A vulnerability classified as problematic has been found in SourceCodester Simple Cold Storage Management System 1.0. Affected is an unknown function of the file /csms/?page=contact_us of the component Contact Us. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-211194 is the identifier assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21592	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.7.39 and prior and 8.0.29 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2022-21589	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.39 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2022-39402	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell: Core Client). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Shell executes to compromise MySQL Shell. While the vulnerability is in MySQL Shell, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Shell accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N).	4.3	More Details
CVE-2022-3582	A vulnerability has been found in SourceCodester Simple Cold Storage Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument change password leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-211189 was assigned to this vulnerability.	4.3	More Details
CVE-2022-39419	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java VM accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2022-3126	The Frontend File Manager Plugin WordPress plugin before 21.4 does not have CSRF check when uploading files, which could allow attackers to make logged in users upload files on their behalf	4.3	More Details
CVE-2022-3464	A vulnerability classified as problematic has been found in puppyCMS up to 5.1. This affects an unknown part of the file /admin/settings.php. The manipulation of the argument site_name leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-210699.	4.3	More Details
CVE-2022-39229	Grafana is an open source data visualization platform for metrics, logs, and traces. Versions prior to 9.1.8 and 8.5.14 allow one user to block another user's login attempt by registering someone else'e email address as a username. A Grafana user's username and email address are unique fields, that means no other user can have the same username or email address as another user. A user can have an email address as a username. However, the login system allows users to log in with either username or email address. Since Grafana allows a user to log in with either their username or email address, this creates an usual behavior where `user_1` can register with one email address and `user_2` can register their username as `user_1``s email address. This prevents `user_1` logging into the application since `user_1``s password won't match with `user_2``s email address. Versions 9.1.8 and 8.5.14 contain a patch. There are no workarounds for this issue.	4.3	More Details
CVE-2022-42159	D-Link COVR 1200,1202,1203 v1.08 was discovered to have a predictable seed in a Pseudo-Random Number Generator.	4.3	More Details
CVE-2022-28887	Multiple Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure products whereby the aerdl.dll unpacker handler function crashes. This can lead to a possible scanning engine crash.	4.3	More Details
CVE-2022-2630	An improper access control issue in GitLab CE/EE affecting all versions starting from 15.2 before 15.2.4, all versions from 15.3 before 15.3.2 allows disclosure of confidential information via the Incident timeline events.	4.3	More Details
CVE-2022-2908	A potential DoS vulnerability was discovered in Gitlab CE/EE versions starting from 10.7 before 15.1.5, all versions starting from 15.2 before 15.2.3, all versions starting from 15.3 before 15.3.1 allowed an attacker to trigger high CPU usage via a special crafted input added in the Commit message field.	4.3	More Details
CVE-2022-3030	An improper access control issue in GitLab CE/EE affecting all versions starting before 15.1.6, all versions from 15.2 before 15.2.4, all versions from 15.3 before 15.3.2 allows disclosure of pipeline status to unauthorized users.	4.3	More Details
CVE-2022-3282	The Drag and Drop Multiple File Upload WordPress plugin before 1.3.6.5 does not properly check for the upload size limit set in forms, taking the value from user input sent when submitting the form. As a result, attackers could control the file length limit and bypass the limit set by admins in the contact form.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3151	The WP Custom Cursors WordPress plugin before 3.0.1 does not have CSRF check in place when deleting cursors, which could allow attackers to made a logged in admin delete arbitrary cursors via a CSRF attack.	4.3	More Details
CVE-2022-3330	It was possible for a guest user to read a todo targeting an inaccessible note in Gitlab CE/EE affecting all versions from 15.0 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1.	4.3	More Details
CVE-2022-3524	A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function ipv6_renew_options of the component IPv6 Handler. The manipulation leads to memory leak. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211021 was assigned to this vulnerability.	4.3	More Details
CVE-2022-3351	An issue has been discovered in GitLab EE affecting all versions starting from 13.7 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. A user's primary email may be disclosed to an attacker through group member events webhooks.	4.3	More Details
CVE-2022-3171	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above.	4.3	More Details
CVE-2022-42067	Online Birth Certificate Management System version 1.0 suffers from an Insecure Direct Object Reference (IDOR) vulnerability	4.3	More Details
CVE-2022-22243	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2.	4.3	More Details
CVE-2022-22245	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2.	4.3	More Details
CVE-2022-35611	A Cross-Site Request Forgery (CSRF) in MQTTRoute v3.3 and below allows attackers to create and remove dashboards.	4.3	More Details
CVE-2022-3244	The Import all XML, CSV & TXT WordPress plugin before 6.5.8 does not have authorisation in some places, which could allow any authenticated users to access some of the plugin features if they manage to get the related nonce	4.2	More Details
CVE-2022-39404	Vulnerability in the MySQL Installer product of Oracle MySQL (component: Installer: General). Supported versions that are affected are 1.6.3 and prior. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Installer executes to compromise MySQL Installer. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Installer accessible data as well as unauthorized read access to a subset of MySQL Installer accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Installer. CVSS 3.1 Base Score 4.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L).	4.2	More Details
CVE-2022-21611	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.30 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.1	More Details
CVE-2022-32491	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39403	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell: Core Client). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Shell executes to compromise MySQL Shell. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Shell accessible data as well as unauthorized read access to a subset of MySQL Shell accessible data. CVSS 3.1 Base Score 3.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N).	3.9	More Details
CVE-2022-21624	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details
CVE-2022-3031	An issue has been discovered in GitLab CE/EE affecting all versions before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. It may be possible for an attacker to guess a user's password by brute force by sending crafted requests to a specific endpoint, even if the victim user has 2FA enabled on their account.	3.7	More Details
CVE-2022-21619	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details
CVE-2022-39399	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details
CVE-2022-3595	A vulnerability was found in Linux Kernel. It has been rated as problematic. Affected by this issue is the function sess_free_buffer of the file fs/cifs/sess.c of the component CIFS Handler. The manipulation leads to double free. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211364.	3.5	More Details
CVE-2022-3533	A vulnerability was found in Linux Kernel. It has been rated as problematic. This issue affects the function parse_usdt_arg of the file tools/lib/bpf/usdt.c of the component BPF. The manipulation of the argument reg_name leads to memory leak. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211031.	3.5	More Details
CVE-2022-39282	FreeRDP is a free remote desktop protocol library and clients. FreeRDP based clients on unix systems using `/parallel` command line switch might read uninitialized data and send it to the server the client is currently connected to. FreeRDP based server implementations are not affected. Please upgrade to 2.8.1 where this issue is patched. If unable to upgrade, do not use parallel port redirection (`/parallel` command line switch) as a workaround.	3.5	More Details
CVE-2022-3331	An issue has been discovered in GitLab EE affecting all versions starting from 14.5 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. GitLab's Zentao integration has an insecure direct object reference vulnerability that may be exploited by an attacker to leak Zentao project issues.	3.5	More Details
CVE-2022-3587	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component My Account. The manipulation of the argument First Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-211201 was assigned to this vulnerability.	3.5	More Details
CVE-2022-3493	A vulnerability, which was classified as problematic, has been found in SourceCodester Human Resource Management System 1.0. This issue affects some unknown processing of the component Add Employee Handler. The manipulation of the argument First Name/Middle Name/Last Name leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-210773 was assigned to this vulnerability.	3.5	More Details
CVE-2022-3553	A vulnerability, which was classified as problematic, was found in X.org Server. This affects an unknown part of the file hw/xquartz/X11Controller.m of the component xquartz. The manipulation leads to denial of service. It is recommended to apply a patch to fix this issue. The identifier VDB-211053 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3505	A vulnerability was found in SourceCodester Sanitization Management System. It has been classified as problematic. Affected is an unknown function of the file /php-sms/admin/. The manipulation of the argument page leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-210840.	3.5	More Details
CVE-2022-3501	Article template contents with sensitive data could be accessed from agents without permissions.	3.5	More Details
CVE-2022-3503	A vulnerability was found in SourceCodester Purchase Order Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the component Supplier Handler. The manipulation of the argument Supplier Name/Address/Contact person/Contact leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-210832.	3.5	More Details
CVE-2022-3502	A vulnerability was found in Human Resource Management System 1.0. It has been classified as problematic. This affects an unknown part of the component Leave Handler. The manipulation of the argument Reason leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-210831.	3.5	More Details
CVE-2022-3497	A vulnerability was found in SourceCodester Human Resource Management System 1.0. It has been classified as problematic. Affected is an unknown function of the component Master List. The manipulation of the argument city/state/country/position leads to cross site scripting. It is possible to launch the attack remotely. VDB-210786 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-3293	Email addresses were leaked in WebHook logs in GitLab EE affecting all versions from 9.3 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1	3.5	More Details
CVE-2022-3288	A branch/tag name confusion in GitLab CE/EE affecting all versions prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an attacker to manipulate pages where the content of the default branch would be expected.	3.5	More Details
CVE-2022-3563	A vulnerability classified as problematic has been found in Linux Kernel. Affected is the function read_50_controller_cap_complete of the file tools/mgmt-tester.c of the component BlueZ. The manipulation of the argument cap_len leads to null pointer dereference. It is recommended to apply a patch to fix this issue. VDB-211086 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-3543	A vulnerability, which was classified as problematic, has been found in Linux Kernel. This issue affects the function unix_sock_destructor/unix_release_sock of the file net/unix/af_unix.c of the component BPF. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211043.	3.5	More Details
CVE-2022-3544	A vulnerability, which was classified as problematic, was found in Linux Kernel. Affected is the function damon_sysfs_add_target of the file mm/damon/sysfs.c of the component Netfilter. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211044.	3.5	More Details
CVE-2017-7517	An input validation vulnerability exists in Openshift Enterprise due to a 1:1 mapping of tenants in Hawkular Metrics and projects/namespaces in OpenShift. If a user creates a project called "MyProject", and then later deletes it another user can then create a project called "MyProject" and access the metrics stored from the original "MyProject" instance.	3.5	More Details
CVE-2022-3551	A vulnerability, which was classified as problematic, has been found in X.org Server. Affected by this issue is the function ProcXkbGetKbdByName of the file xkb/xkb.c. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211052.	3.5	More Details
CVE-2022-41597	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.	3.4	More Details
CVE-2022-41603	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.	3.4	More Details
CVE-2022-41600	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.	3.4	More Details
CVE-2022-41598	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.	3.4	More Details
CVE-2022-41592	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.	3.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41595	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.	3.4	More Details
CVE-2022-41594	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.	3.4	More Details
CVE-2022-41593	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.	3.4	More Details
CVE-2022-41601	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.	3.4	More Details
CVE-2022-41602	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.	3.4	More Details
CVE-2022-21610	Vulnerability in the Oracle Solaris product of Oracle Systems (component: LDoms). The supported version that is affected is 11. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 3.3 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:L).	3.3	More Details
CVE-2022-3325	Improper access control in the GitLab CE/EE API affecting all versions starting from 12.8 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. Allowed for editing the approval rules via the API by an unauthorised user.	2.7	More Details
CVE-2022-3279	An unhandled exception in job log parsing in GitLab CE/EE affecting all versions prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an attacker to prevent access to job logs	2.7	More Details
CVE-2022-39409	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Business Process Automation). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Transportation Management. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.7	More Details
CVE-2022-3521	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function kcm_tx_work of the file net/kcm/kcmsock.c of the component kcm. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. VDB-211018 is the identifier assigned to this vulnerability.	2.6	More Details
CVE-2022-3581	A vulnerability, which was classified as problematic, was found in SourceCodester Cashier Queuing System 1.0. Affected is an unknown function of the component Cashiers Tab. The manipulation of the argument Name leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-211188.	2.4	More Details
CVE-2022-3580	A vulnerability, which was classified as problematic, has been found in SourceCodester Cashier Queuing System 1.0.1. This issue affects some unknown processing of the component User Creation Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-211187.	2.4	More Details
CVE-2022-3546	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /csms/admin/?page=user/list of the component Create User Handler. The manipulation of the argument First Name/Last Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-211046 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2022-3548	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the component Add New Storage Handler. The manipulation of the argument Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-211048.	2.4	More Details
CVE-2022-3518	A vulnerability classified as problematic has been found in SourceCodester Sanitization Management System 1.0. Affected is an unknown function of the component User Creation Handler. The manipulation of the argument First Name/Middle Name/Last Name leads to cross site scripting. It is possible to launch the attack remotely. VDB-211014 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2022-3547	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /csms/admin/?page=system_info of the component Setting Handler. The manipulation of the argument System Name/System Short Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-211047.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3519	A vulnerability classified as problematic was found in SourceCodester Sanitization Management System 1.0. Affected by this vulnerability is an unknown functionality of the component Quote Requests Tab. The manipulation of the argument Manage Remarks leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-211015.	2.4	More Details
CVE-2020-26863	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2022-3554	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-3593	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-3555	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2020-26851	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26866	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26865	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26864	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-35539	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-3528	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2020-26850	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26861	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26860	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26859	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26858	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26857	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26856	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26855	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26854	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26862	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26849	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2022-3529	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2020-26848	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26839	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26840	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26841	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26842	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26843	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26844	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26845	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2022-3530	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-3531	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-3532	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-3535	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2020-26853	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3542	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-3527	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2020-26846	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2020-26847	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details
CVE-2022-3522	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2020-26852	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none.	N/A	More Details