SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 July 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-2022-31161	Roxy-WI is a Web interface for managing HAProxy, Nginx and Keepalived servers. Prior to version 6.1.1.0, the system command can be run remotely via the subprocess_execute function without processing the inputs received from the user in the /app/options.py file. Version 6.1.1.0 contains a patch for this issue.	10.0	More Details
CVE-2022-32073	WolfSSH v1.4.7 was discovered to contain an integer overflow via the function wolfSSH_SFTP_RecvRMDIR.	9.8	More Details
CVE-2022-27434	UNIT4 TETA Mobile Edition (ME) before 29.5.HF17 was discovered to contain a SQL injection vulnerability via the ProfileName parameter in the errorReporting page.	9.8	More Details
CVE-2022-31209	An issue was discovered in Infiray IRAY-A8Z3 1.0.957. The firmware contains a potential buffer overflow by calling strcpy() without checking the string length beforehand.	9.8	More Details
CVE-2022-31210	An issue was discovered in Infiray IRAY-A8Z3 1.0.957. The binary file /usr/local/sbin/webproject/set_param.cgi contains hardcoded credentials to the web application. Because these accounts cannot be deactivated or have their passwords changed, they are considered to be backdoor accounts.	9.8	More Details
CVE-2022-31211	An issue was discovered in Infiray IRAY-A8Z3 1.0.957. There is a blank root password for TELNET by default.	9.8	More Details
CVE-2022-32985	libnx_apl.so on Nexans FTTO GigaSwitch before 6.02N and 7.x before 7.02 implements a Backdoor Account for SSH logins on port 50200 or 50201.	9.8	More Details
CVE-2021-40874	An issue was discovered in LemonLDAP::NG (aka lemonldap-ng) 2.0.13. When using the RESTServer plug-in to operate a REST password validation service (for another LemonLDAP::NG instance, for example) and using the Kerberos authentication method combined with another method with the Combination authentication plug-in, any password will be recognized as valid for an existing user.	9.8	More Details
CVE-2021-41419	QVIS NVR DVR before 2021-12-13 is vulnerable to Remote Code Execution via Java deserialization.	9.8	More Details
CVE-2022-35741	Apache CloudStack version 4.5.0 and later has a SAML 2.0 authentication Service Provider plugin which is found to be vulnerable to XML external entity (XXE) injection. This plugin is not enabled by default and the attacker would require that this plugin be enabled to exploit the vulnerability. When the SAML 2.0 plugin is enabled in affected versions of Apache CloudStack could potentially allow the exploitation of XXE vulnerabilities. The SAML 2.0 messages constructed during the authentication flow in Apache CloudStack are XML-based and the XML data is parsed by various standard libraries that are now understood to be vulnerable to XXE injection attacks such as arbitrary file reading, possible denial of service, server-side request forgery (SSRF) on the CloudStack management server.	9.8	More Details
CVE-2022-28888	Spryker Commerce OS 1.4.2 allows Remote Command Execution.	9.8	More Details
CVE-2022-2437	The Feed Them Social – for Twitter feed, Youtube and more plugin for WordPress is vulnerable to deserialization of untrusted input via the 'fts_url' parameter in versions up to, and including 2.9.8.5. This makes it possible for unauthenticated attackers to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.	9.8	More Details
CVE-2015-8031	Hudson (aka org.jvnet.hudson.main:hudson-core) before 3.3.2 allows XXE attacks.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34635	The mstatus.sd field in CVA6 commit d315ddd0f1be27c1b3f27eb0b8daf471a952299a does not update when the mstatus.fs field is set to Dirty.	9.8	More Details
CVE-2022-24082	If an on-premise installation of the Pega Platform is configured with the port for the JMX interface exposed to the Internet and port filtering is not properly configured, then it may be possible to upload serialized payloads to attack the underlying system. This does not affect systems running on PegaCloud due to its design and architecture.	9.8	More Details
CVE-2022-35405	Zoho ManageEngine Password Manager Pro before 12101 and PAM360 before 5510 are vulnerable to unauthenticated remote code execution. (This also affects ManageEngine Access Manager Plus before 4303 with authentication.)	9.8	More Details
CVE-2022-35912	In grails-databinding in Grails before 3.3.15, 4.x before 4.1.1, 5.x before 5.1.9, and 5.2.x before 5.2.1 (at least when certain Java 8 configurations are used), data binding allows a remote attacker to execute code by gaining access to the class loader.	9.8	More Details
CVE-2022-34023	Barangay Management System v1.0 was discovered to contain a SQL injection vulnerability via the hidden_id parameter at /officials/officials.php.	9.8	More Details
CVE-2022-26479	An issue was discovered in Poly EagleEye Director II before 2.2.2.1. Existence of a certain file (which can be created via an rsync backdoor) causes all API calls to execute as admin without authentication.	9.8	More Details
CVE-2022-26352	An issue was discovered in the ContentResource API in dotCMS 3.0 through 22.02. Attackers can craft a multipart form request to post a file whose filename is not initially sanitized. This allows directory traversal, in which the file is saved outside of the intended storage location. If anonymous content creation is enabled, this allows an unauthenticated attacker to upload an executable file, such as a .jsp file, that can lead to remote code execution.	9.8	More Details
CVE-2021-36711	WebInterface in OctoBot before 0.4.4 allows remote code execution because Tentacles upload is mishandled.	9.8	More Details
CVE-2022-28369	Verizon 5G Home LVSKIHP InDoorUnit (IDU) 3.4.66.162 does not validate the user-provided URL within the crtcmode function's enable_ssh sub-operation of the crtcrpc JSON listener (found at /lib/functions/wnc_jsonsh/crtcmode.sh) A remote attacker on the local network can provide a malicious URL. The data (found at that URL) is written to /usr/sbin/dropbear and then executed as root.	9.8	More Details
CVE-2022-20216	android exported is used to set third-party app access permissions, and the default value of intent-filter is true. com.sprd.firewall has set exported as true.Product: AndroidVersions: Android SoCAndroid ID: A-231911916	9.8	More Details
CVE-2022-20222	In read_attr_value of gatt_db.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-228078096	9.8	More Details
CVE-2022-20229	In bta_hf_client_handle_cind_list_item of bta_hf_client_at.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-224536184	9.8	More Details
CVE-2022-20238	'remap_pfn_range' here may map out of size kernel memory (for example, may map the kernel area), and because the 'vma->vm_page_prot' can also be controlled by userspace, so userspace may map the kernel area to be writable, which is easy to be exploitedProduct: AndroidVersions: Android SoCAndroid ID: A-233154555	9.8	More Details
CVE-2022-35857	kvf-admin through 2022-02-12 allows remote attackers to execute arbitrary code because deserialization is mishandled. The rememberMe parameter is encrypted with a hardcoded key from the com.kalvin.kvf.common.shiro.ShiroConfig file.	9.8	More Details
CVE-2022-35890	An issue was discovered in Inductive Automation Ignition before 7.9.20 and 8.x before 8.1.17. Designer and Vision Client Session IDs are mishandled. An attacker can determine which session IDs were generated in the past and then hijack sessions assigned to these IDs via Randy.	9.8	More Details
CVE-2022-21543	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Updates Environment Mgmt). Supported versions that are affected are 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. 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-2022-28373	Verizon 5G Home LVSKIHP InDoorUnit (IDU) 3.4.66.162 does not properly sanitize user-controlled parameters within the crtcreadpartition function of the crtcrpc JSON listener in /usr/lib/lua/luci/crtc.lua. A remote attacker on the local network can inject shell metacharacters to achieve remote code execution as root.	9.8	More Details
CVE-2022-28375	Verizon 5G Home LVSKIHP OutDoorUnit (ODU) 3.33.101.0 does not property sanitize user-controlled parameters within the crtcswitchsimprofile function of the crtcrpc JSON listener. A remote attacker on the local network can inject shell metacharacters into /usr/lib/lua/5.1/luci/controller/rpc.lua to achieve remote code execution as root,	9.8	More Details
CVE-2022-30113	Electronic mall system 1.0_build20200203 is affected vulnerable to SQL Injection.	9.8	More Details
CVE-2022-32409	A local file inclusion (LFI) vulnerability in the component codemirror.php of Portal do Software Publico Brasileiro i3geo v7.0.5 allows attackers to execute arbitrary PHP code via a crafted HTTP request.	9.8	More Details
CVE-2022-32417	PbootCMS v3.1.2 was discovered to contain a remote code execution (RCE) vulnerability via the function parserIfLabel at function.php.	9.8	More Details
CVE-2022-25800	Best Practical RT for Incident Response (RTIR) before 4.0.3 and 5.x before 5.0.3 allows SSRF via the whois lookup tool.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34029	Nginx NJS v0.7.4 was discovered to contain an out-of-bounds read via njs_scope_value at njs_scope.h.	9.1	More Details
CVE-2022-34632	Rocket-Chip commit 4f8114374d8824dfdec03f576a8cd68bebce4e56 was discovered to contain insufficient cryptography via the component /rocket/RocketCore.scala.	9.1	More Details
CVE-2022-35409	An issue was discovered in Mbed TLS before 2.28.1 and 3.x before 3.2.0. In some configurations, an unauthenticated attacker can send an invalid ClientHello message to a DTLS server that causes a heap-based buffer over-read of up to 255 bytes. This can cause a server crash or possibly information disclosure based on error responses. Affected configurations have MBEDTLS_SSL_DTLS_CLIENT_PORT_REUSE enabled and MBEDTLS_SSL_IN_CONTENT_LEN less than a threshold that depends on the configuration: 258 bytes if using mbedtls_ssl_cookie_check, and possibly up to 571 bytes with a custom cookie check function.	9.1	More Details
CVE-2022-25801	Best Practical RT for Incident Response (RTIR) before 4.0.3 and 5.x before 5.0.3 allows SSRF via Scripted Action tools.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2022-32114	An unrestricted file upload vulnerability in the Add New Assets function of Strapi 4.1.12 allows attackers to conduct XSS attacks via a crafted PDF file. NOTE: the project documentation suggests that a user with the Media Library "Create (upload)" permission is supposed to be able to upload PDF files containing JavaScript, and that all files in a public assets folder are accessible to the outside world (unless the filename begins with a dot character). The administrator can choose to allow only image, video, and audio files (i.e., not PDF) if desired.
CVE-2022-2001	The DX Share Selection plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.4. This is due to missing nonce protection on the dxss_admin_page() function found in the ~/dx-share-selection.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site's administrator into performing an action such as clicking on a link.
CVE-2022-30243	Honeywell Alerton Visual Logic through 2022-05-04 allows unauthenticated programming writes from remote users. This enables code to be stored on the controller and then run without verification. A user with malicious intent can send a crafted packet to change and/or stop the program without the knowledge of other users, altering the controller's function. After the programming change, the program needs to be overwritten in order for the controller to restore its original operational function.
CVE-2022-26481	An issue was discovered in Poly Studio before 3.7.0. Command Injection can occur via the CN field of a Create Certificate Signing Request (CSR) action.
CVE-2022-1912	The Button Widget Smartsoft plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.1. This is due to missing nonce validation on the smartsoftbutton_settings page. This makes it possible for unauthenticated attackers to update the plugins settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2022-34538	Digital Watchdog DW MEGApix IP cameras A7.2.2_20211029 was discovered to contain a command injection vulnerability in the component /admin/vca/bia/addacph.cgi. This vulnerability is exploitable via a crafted POST request.
CVE-2022-1672	The Insights from Google PageSpeed WordPress plugin before 4.0.7 does not verify for CSRF before doing various actions such as deleting Custom URLs, which could allow attackers to make a logged in admin perform such actions via CSRF attacks
CVE-2022-34756	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could result in remote code execution or the crash of HTTPs stack which is used for the device Web HMI. Affected Products: Easergy P5 (V01.401.102 and prior)
CVE-2022-30550	An issue was discovered in the auth component in Dovecot 2.2 and 2.3 before 2.3.20. When two passdb configuration entries exist with the same driver and args settings, incorrect username_filter and mechanism settings can be applied to passdb definitions. These incorrectly applied settings can lead to an unintended security configuration and can permit privilege escalation in certain configurations. The documentation does not advise against the use of passdb definitions that have the same driver and args settings. One such configuration would be where an administrator wishes to use the same PAM configuration or passwd file for both normal and master users but use the username_filter setting to restrict which of the users is able to be a master user.
CVE-2022-26117	An empty password in configuration file vulnerability [CWE-258] in FortiNAC version 8.3.7 and below, 8.5.2 and below, 8.5.4, 8.6.0, 8.6.5 and below, 8.7.6 and below, 8.8.11 and below, 9.1.5 and below, 9.2.3 and below may allow an authenticated attacker to access the MySQL databases via the CLI.
CVE-2022-34753	A CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could cause remote root exploit when the command is compromised. Affected Products: SpaceLogic C-Bus Home Controller (5200WHC2), formerly known as C-Bus Wiser Homer Controller MK2 (V1.31.460 and prior)
CVE-2022-32320	A Cross-Site Request Forgery (CSRF) in Ferdi through 5.8.1 and Ferdium through 6.0.0-nightly.98 allows attackers to read files via an uploaded file such as a settings/preferences file.
CVE-2022-2039	The Free Live Chat Support plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.0.11. This is due to missing nonce protection on the livesupporti_settings() function found in the ~/livesupporti.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site's administrator into performing an action such as clicking on a link.

CVE Number	Description
CVE-2022-2435	The AnyMind Widget plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.1. This is due to missing nonce protection on the createDOMStructure() function found in the ~/anymind-widget-id.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site's administrator into performing an action such as clicking on a link.
CVE-2022-2443	The FreeMind WP Browser plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.2. This is due to missing nonce protection on the FreemindOptions() function found in the ~/freemind-wp-browser.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site's administrator into performing an action such as clicking on a link.
CVE-2022-2444	The Visualizer: Tables and Charts Manager for WordPress plugin for WordPress is vulnerable to deserialization of untrusted input via the 'remote_data' parameter in versions up to, and including 3.7.9. This makes it possible for authenticated attackers with contributor privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.
CVE-2021-36461	An Arbitrary File Upload vulnerability exists in Microweber 1.1.3 that allows attackers to getshell via the Settings Upload Picture section by uploading pictures with malicious code, user.ini.
CVE-2022-30981	An issue was discovered in Gentics CMS before 5.43.1. By uploading a malicious ZIP file, an attacker is able to deserialize arbitrary data and hence can potentially achieve Java code execution.
CVE-2022-22360	IBM Sterling Partner Engagement Manager 6.1.2, 6.2, and Cloud/SasS 22.2 could allow a remote authenticated attacker to conduct an LDAP injection. By using a specially crafted request, an attacker could exploit this vulnerability and could result in in granting permission to unauthorized resources. IBM X-Force ID: 220782.
CVE-2022-31208	An issue was discovered in Infiray IRAY-A8Z3 1.0.957. The webserver contains an endpoint that can execute arbitrary commands by manipulating the cmd_string URL parameter.
CVE-2022-27373	Shanghai Feixun Data Communication Technology Co., Ltd router fir302b A2 was discovered to contain a remote command execution (RCE) vulnerability via the Ping function.
CVE-2022-34539	Digital Watchdog DW MEGApix IP cameras A7.2.2_20211029 was discovered to contain a command injection vulnerability in the component /admin/curltest.cgi. This vulnerability is exploitable via a crafted POST request.
CVE-2022-34540	Digital Watchdog DW MEGApix IP cameras A7.2.2_20211029 was discovered to contain a command injection vulnerability in the component /admin/vca/license/license_tok.cgi. This vulnerability is exploitable via a crafted POST request.
CVE-2022-32415	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/?p=products/view_product&id=.
CVE-2022-33891	The Apache Spark UI offers the possibility to enable ACLs via the configuration option spark.acls.enable. With an authentication filter, this checks whether a user has access permissions to view or modify the application. If ACLs are enabled, a code path in HttpSecurityFilter can allow someone to perform impersonation by providing an arbitrary user name. A malicious user might then be able to reach a permission check function that will ultimately build a Unix shell command based on their input, and execute it. This will result in arbitrary shell command execution as the user Spark is currently running as. This affects Apache Spark versions 3.0.3 and earlier, versions 3.1.1 to 3.1.2, and versions 3.2.0 to 3.2.1.
CVE-2022-24688	An issue was discovered in DSK DSKNet 2.16.136.0 and 2.17.136.5. The Touch settings allow unrestricted file upload (and consequently Remote Code Execution) via PDF upload with PHP content and a .php extension. The attacker must hijack or obtain privileged user access to the Parameters page in order to exploit this issue. (That can be easily achieved by exploiting the Broken Access Control with further Brute-force attack or SQL Injection.) The uploaded file is stored within the database and copied to the sync web folder if the attacker visits a certain .php?action= page.
CVE-2022-28374	Verizon 5G Home LVSKIHP OutDoorUnit (ODU) 3.33.101.0 does not property sanitize user-controlled parameters within the DMACC URLs on the Settings page of the Engineering portal. An authenticated remote attacker on the local network can inject shell metacharacters into /usr/lib/lua/5.1/luci/controller/admin/settings.lua to achieve remote code execution as root.
CVE-2022-30024	A buffer overflow in the httpd daemon on TP-Link TL-WR841N V12 (firmware version 3.16.9) devices allows an authenticated remote attacker to execute arbitrary code via a GET request to the page for the System Tools of the Wi-Fi network. This affects TL-WR841 V12 TL-WR841N(EU)_V12_160624 and TL-WR841 V11 TL-WR841N(EU)_V11_160325 , TL-WR841N_V11_150616 and TL-WR841 V10 TL-WR841N_V10_150310 are also affected.
CVE-2022-34890	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 17.1.1 (51537). An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Parallels Tools component. The issue results from the lack of proper validation of a user-supplied value prior to dereferencing it as a pointer. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the kernel. Was ZDI-CAN-16653.
CVE-2022-21510	Vulnerability in the Oracle Database - Enterprise Edition Sharding component of Oracle Database Server. For supported versions that are affected see note. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Oracle Database - Enterprise Edition Sharding executes to compromise Oracle Database - Enterprise Edition Sharding. While the vulnerability is in Oracle Database - Enterprise Edition Sharding, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Database - Enterprise Edition Sharding. Note: None of the supported versions are affected. 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).

CVE Number	Description
CVE-2022-32119	Arox School ERP Pro v1.0 was discovered to contain multiple arbitrary file upload vulnerabilities via the Add Photo function at photogalleries.inc.php and the import staff excel function at 1finance_master.inc.php.
CVE-2019-10761	This affects the package vm2 before 3.6.11. It is possible to trigger a RangeError exception from the host rather than the "sandboxed" context by reaching the stack call limit with an infinite recursion. The returned object is then used to reference the mainModule property of the host code running the script allowing it to spawn a child_process and execute arbitrary code.
CVE-2021-34987	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.5.1 (49187). An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the HDAudio virtual device. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-14969.
CVE-2022-21513	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. While the vulnerability is in Oracle ZFS Storage Appliance Kit, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2022-35404	ManageEngine Password Manager Pro 12100 and prior and OPManager 126100 and prior are vulnerable to unauthorized file and directory creation on a server machine.
CVE-2022-27933	Pexip Infinity before 27.3 allows remote attackers to trigger a software abort via One Touch Join.
CVE-2022-30620	On Cellinx Camera with guest enabled, attacker with web access can elevate privileges to administrative: "1" to "0" privileges by changing the following cookie values from "is_admin", "showConfig". Administrative Privileges which allows changing various configuration in the camera.
CVE-2022-21571	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.36. 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 takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2022-24690	An issue was discovered in DSK DSKNet 2.16.136.0 and 2.17.136.5. A PresAbs.php SQL Injection vulnerability allows unauthenticated users to taint database data and extract sensitive information via crafted HTTP requests. The type of SQL Injection is blind boolean based. (An unauthenticated attacker can discover the endpoint by abusing a Broken Access Control issue with further SQL injection attacks to gather all user's badge numbers and PIN codes.)
CVE-2022-34889	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 17.1.1 (51537). An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the ACPI virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-16554.
CVE-2022-26656	Pexip Infinity before 27.3 allows remote attackers to trigger a software abort, and possibly enumerate usernames, via One Touch Join.
CVE-2022-21429	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Billing Care). Supported versions that are affected are 12.0.0.4.0-12.0.0.6.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. 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).
CVE-2022-29060	A use of hard-coded cryptographic key vulnerability [CWE-321] in FortiDDoS API 5.5.0 through 5.5.1, 5.4.0 through 5.4.2, 5.3.0 through 5.3.1, 5.2.0, 5.1.0 may allow an attacker who managed to retrieve the key from one device to sign JWT tokens for any device.
CVE-2022-32212	A OS Command Injection vulnerability exists in Node.js versions <14.20.0, <16.20.0, <18.5.0 due to an insufficient IsAllowedHost check that can easily be bypassed because IsIPAddress does not properly check if an IP address is invalid before making DBS requests allowing rebinding attacks.
CVE-2022-21536	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Policy Framework). Supported versions that are affected are 13.4.0.0 and 13.5.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Enterprise Manager Base Platform. 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).
CVE-2022-2420	A vulnerability was found in URVE Web Manager. It has been rated as critical. This issue affects some unknown processing of the file _internal/uploader.php. The manipulation leads to unrestricted upload. The attack needs to be approached within the local network. The exploit has been disclosed to the public and may be used.
CVE-2022-2418	A vulnerability was found in URVE Web Manager. It has been classified as critical. This affects an unknown part of the file kreator.html5/img_upload.php. The manipulation leads to unrestricted upload. Access to the local network is required for this attack. The exploit has been disclosed to the public and may be used.

CVE Number	Description
CVE-2022-2419	A vulnerability was found in URVE Web Manager. It has been declared as critical. This vulnerability affects unknown code of the file _internal/collector/upload.php. The manipulation leads to unrestricted upload. Access to the local network is required for this attack to succeed. The exploit has been disclosed to the public and may be used.
CVE-2022-30244	Honeywell Alerton Ascent Control Module (ACM) through 2022-05-04 allows unauthenticated programming writes from remote users. This enables code to be store on the controller and then run without verification. A user with malicious intent can send a crafted packet to change and/or stop the program without the knowledge of other users, altering the controller's function. After the programming change, the program needs to be overwritten in order for the controller to restore its original operational function.
CVE-2022-31159	The AWS SDK for Java enables Java developers to work with Amazon Web Services. A partial-path traversal issue exists within the `downloadDirectory` method in the AWS S3 TransferManager component of the AWS SDK for Java v1 prior to version 1.12.261. Applications using the SDK control the `destinationDirectory` argument, but S3 object keys are determined by the application that uploaded the objects. The `downloadDirectory` method allows the caller to pass a filesystem object in the object key but contained an issue in the validation logic for the key name. A knowledgeable actor could bypass the validation logic by including a UNIX double-dot in the bucket key. Under certain conditions, this could permit them to retrieve a directory from their S3 bucket that is one level up in the filesystem from their working directory. This issue's scope is limited to directories whose name prefix matches the destinationDirectory. E.g. for destination directory`/tmp/foo`, the actor can cause a download to `/tmp/foo-bar`, but not `/tmp/bar`. If `com.amazonaws.services.s3.transfer.TransferManager::downloadDirectory` is used to download an untrusted buckets contents, the contents of that bucket can be written outside of the intended destination directory. Version 1.12.261 contains a patch for this issue. As a workaround, when calling `com.amazonaws.services.s3.transfer.TransferManager::downloadDirectory`, pass a `KeyFilter` that forbids `S3ObjectSummary` objects that `getKey` method return a string containing the substring `..` .
CVE-2022-30301	A path traversal vulnerability [CWE-22] in FortiAP-U CLI 6.2.0 through 6.2.3, 6.0.0 through 6.0.4, 5.4.0 through 5.4.6 may allow an admin user to delete and access unauthorized files and data via specifically crafted CLI commands.
CVE-2022-34230	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-2454	Integer Overflow or Wraparound in GitHub repository gpac/gpac prior to 2.1-DEV.
CVE-2022-2453	Use After Free in GitHub repository gpac/gpac prior to 2.1-DEV.
CVE-2022-34242	Adobe Character Animator version 4.4.7 (and earlier) and 22.4 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34226	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34229	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34228	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by an Access of Uninitialized Pointer 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.
CVE-2022-27580	A deserialization vulnerability in a .NET framework class used and not properly checked by Safety Designer all versions up to and including 1.11.0 allows an attacker to craft malicious project files. Opening/importing such a malicious project file would execute arbitrary code with the privileges of the current user when opened or imported by the Safety Designer. This compromises confidentiality integrity and availability. For the attack to succeed a user must manually open a malicious project file.
CVE-2022-34225	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34223	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34222	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34220	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-1920	Integer overflow in matroskademux element in gst_matroska_demux_add_wvpk_header function which allows a heap overwrite while parsing matroska files. Potential for arbitrary code execution through heap overwrite.

CVE Number	Description
CVE-2022-34219	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34217	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by an Out-Of-Bounds Write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34216	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34215	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-27579	A deserialization vulnerability in a .NET framework class used and not properly checked by Flexi Soft Designer in all versions up to and including 1.9.4 SP1 allows an attacker to craft malicious project files. Opening/importing such a malicious project file would execute arbitrary code with the privileges of the current user when opened or imported by the Flexi Soft Designer. This compromises confidentiality integrity and availability. For the attack to succeed a user must manually open a malicious project file.
CVE-2022-34241	Adobe Character Animator version 4.4.7 (and earlier) and 22.4 (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 requires user interaction in that a victim must open a malicious file.
CVE-2022-32434	EIPStackGroup OpENer v2.3.0 was discovered to contain a stack overflow via /bin/posix/src/ports/POSIX/OpENer+0x56073d.
CVE-2022-34243	Adobe Photoshop versions 22.5.7 (and earlier) and 23.3.2 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34245	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (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 requires user interaction in that a victim must open a malicious file.
CVE-2022-28672	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16640.
CVE-2022-28671	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16639.
CVE-2022-28670	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. Crafted data in an AcroForm can trigger a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-16523.
CVE-2022-28669	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16420.
CVE-2021-41031	A relative path traversal vulnerability [CWE-23] in FortiClient for Windows versions 7.0.2 and prior, 6.4.6 and prior and 6.2.9 and below may allow a local unprivileged attacker to escalate their privileges to SYSTEM via the named pipe responsible for FortiESNAC service.
CVE-2022-35861	pyenv 1.2.24 through 2.3.2 allows local users to gain privileges via a .python-version file in the current working directory. An attacker can craft a Python version string in .python-version to execute shims under their control. (Shims are executables that pass a command along to a specific version of pyenv. The version string is used to construct the path to the command, and there is no validation of whether the version specified is a valid version. Thus, relative path traversal can occur.)
CVE-2022-28807	An issue was discovered in Open Design Alliance Drawings SDK before 2023.2. An Out-of-Bounds Read vulnerability exists when rendering a .dwg file after it's opened in the recovery mode. An attacker can leverage this vulnerability to execute code in the context of the current process.
CVE-2022-28809	An issue was discovered in Open Design Alliance Drawings SDK before 2023.3. An Out-of-Bounds Read vulnerability exists when reading a DWG file with an invalid vertex number in a recovery mode. An attacker can leverage this vulnerability to execute code in the context of the current process.
CVE-2022-34902	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Access 6.5.4 (39316) Agent. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Desktop Control Agent service. The service loads Qt plugins from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-15787.

CVE Number	Description
CVE-2022-34901	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Access 6.5.4 (39316) Agent. An attacker must first obtain the ability to execute low-privileged code on the target host system in order to exploit this vulnerability. The specific flaw exists within the Parallels Service. The service executes files from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-16137.
CVE-2022-34900	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Access 6.5.3 (39313) Agent. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Dispatcher service. The service loads an OpenSSL configuration file from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-15213.
CVE-2022-34899	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Access 6.5.4 (39316) Agent. An attacker must first obtain the ability to execute low-privileged code on the target host system in order to exploit this vulnerability. The specific flaw exists within the Parallels service. By creating a symbolic link, an attacker can abuse the service to execute a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-16134.
CVE-2021-44954	In QVIS NVR DVR before 2021-12-13, an attacker can escalate privileges from a qvisdvr user to the root user by abusing a Sudo misconfiguration.
CVE-2022-34892	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop Parallels Desktop 17.1.1. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the update machanism. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-16396.
CVE-2022-34891	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop Parallels Desktop 17.1.1. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the update machanism. The product sets incorrect permissions on sensitive files. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-16395.
CVE-2022-28673	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16641.
CVE-2022-28674	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16644.
CVE-2022-28675	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16642.
CVE-2022-30526	A privilege escalation vulnerability was identified in the CLI command of Zyxel USG FLEX 100(W) firmware versions 4.50 through 5.30, USG FLEX 200 firmware versions 4.50 through 5.30, USG FLEX 500 firmware versions 4.50 through 5.30, USG FLEX 700 firmware versions 4.50 through 5.30, USG FLEX 50(W) firmware versions 4.16 through 5.30, USG20(W)-VPN firmware versions 4.16 through 5.30, ATP series firmware versions 4.32 through 5.30, VPN series firmware versions 4.30 through 5.30, USG/ZyWALL series firmware versions 4.09 through 4.72, which could allow a local attacker to execute some OS commands with root privileges in some directories on a vulnerable device.
CVE-2022-34246	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (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 requires user interaction in that a victim must open a malicious file.
CVE-2022-34247	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an Out-Of-Bounds Write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34249	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (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 requires user interaction in that a victim must open a malicious file.
CVE-2022-34250	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (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 requires user interaction in that a victim must open a malicious file.
CVE-2022-34251	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an Out-Of-Bounds Write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2021-34986	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.5.0 (49183). An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Parallels Service. By creating a symbolic link, an attacker can abuse the service to execute a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-13932.

CVE Number	Description
CVE-2022-1922	DOS / potential heap overwrite in mkv demuxing using zlib decompression. Integer overflow in matroskademux element in gst_matroska_decompress_data function which causes a segfault, or could cause a heap overwrite, depending on libc and OS. Depending on the libc used, and the underlying OS capabilities, it could be just a segfault or a heap overwrite. If the libc uses mmap for large chunks, and the OS supports mmap, then it is just a segfault (because the realloc before the integer overflow will use mremap to reduce the size of the chunk, and it will start to write to unmapped memory). However, if using a libc implementation that does not use mmap, or if the OS does not support mmap while using libc, then this could result in a heap overwrite.
CVE-2022-28676	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16643.
CVE-2022-28683	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the deletePages method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16828.
CVE-2022-28682	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. By performing actions in JavaScript, an attacker can trigger a read past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16778.
CVE-2022-28680	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16821.
CVE-2022-28679	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16861.
CVE-2022-28678	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16805.
CVE-2022-28677	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16663.
CVE-2022-1921	Integer overflow in avidemux element in gst_avi_demux_invert function which allows a heap overwrite while parsing avi files. Potential for arbitrary code execution through heap overwrite.
CVE-2022-28808	An issue was discovered in Open Design Alliance Drawings SDK before 2023.3. An Out-of-Bounds Read vulnerability exists when reading DWG files in a recovery mode. An attacker can leverage this vulnerability to execute code in the context of the current process.
CVE-2022-1923	DOS / potential heap overwrite in mkv demuxing using bzip decompression. Integer overflow in matroskademux element in bzip decompression function which causes a segfault, or could cause a heap overwrite, depending on libc and OS. Depending on the libc used, and the underlying OS capabilities, it could be just a segfault or a heap overwrite. If the libc uses mmap for large chunks, and the OS supports mmap, then it is just a segfault (because the realloc before the integer overflow will use mremap to reduce the size of the chunk, and it will start to write to unmapped memory). However, if using a libc implementation that does not use mmap, or if the OS does not support mmap while using libc, then this could result in a heap overwrite.
CVE-2021-26384	A malformed SMI (System Management Interface) command may allow an attacker to establish a corrupted SMI Trigger Info data structure, potentially leading to out-of-bounds memory reads and writes when triggering an SMI resulting in a potential loss of resources.
CVE-2022-20212	In wifi.RequestToggleWifiActivity of AndroidManifest.xml, there is a possible EoP due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-182282630
CVE-2022-20218	In PermissionController, there is a possible way to get and retain permissions without user's consent due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-223907044
CVE-2022-20220	In openFile of CallLogProvider.java, there is a possible permission bypass due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-219015884
CVE-2022-20223	In assertSafeToStartCustomActivity of AppRestrictionsFragment.java, there is a possible way to start a phone call without permissions due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-223578534

CVE Number	Description
CVE-2022-32117	Jerryscript v2.4.0 was discovered to contain a stack buffer overflow via the function jerryx_print_unhandled_exception in /util/print.c.
CVE-2022-1924	DOS / potential heap overwrite in mkv demuxing using lzo decompression. Integer overflow in matroskademux element in lzo decompression function which causes a segfault, or could cause a heap overwrite, depending on libc and OS. Depending on the libc used, and the underlying OS capabilities, it could be just a segfault or a heap overwrite. If the libc uses mmap for large chunks, and the OS supports mmap, then it is just a segfault (because the realloc before the integer overflow will use mremap to reduce the size of the chunk, and it will start to write to unmapped memory). However, if using a libc implementation that does not use mmap, or if the OS does not support mmap while using libc, then this could result in a heap overwrite.
CVE-2022-21558	Vulnerability in the Oracle Crystal Ball product of Oracle Construction and Engineering (component: Installation). Supported versions that are affected are 11.1.2.0.000-11.1.2.4.900. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Crystal Ball executes to compromise Oracle Crystal Ball. While the vulnerability is in Oracle Crystal Ball, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Crystal Ball. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).
CVE-2021-45492	In Sage 300 ERP (formerly accpac) through 6.8.x, the installer configures the C:\Sage\Sage300\Runtime directory to be the first entry in the system-wide PATH environment variable. However, this directory is writable by unprivileged users because the Sage installer fails to set explicit permissions and therefore inherits weak permissions from the C:\ folder. Because entries in the system-wide PATH variable are included in the search order for DLLs, an attacker could perform DLL search-order hijacking to escalate their privileges to SYSTEM. Furthermore, if the Global Search or Web Screens functionality is enabled, then privilege escalation is possible via the GlobalSearchService and Sage.CNA.WindowsService services, again via DLL search-order hijacking because unprivileged users would have modify permissions on the application directory. Note that while older versions of the software default to installing in %PROGRAMFILES(X86)% (which would allow the Sage folder to inherit strong permissions, making the installation not vulnerable), the official Sage 300 installation guides for those versions recommend installing in C:\Sage, which would make the installation vulnerable.
CVE-2022-34221	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (and earlier) are affected by an Access of Resource Using Incompatible Type ('Type Confusion') 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.
CVE-2022-1925	DOS / potential heap overwrite in mkv demuxing using HEADERSTRIP decompression. Integer overflow in matroskaparse element in gst_matroska_decompress_data function which causes a heap overflow. Due to restrictions on chunk sizes in the matroskademux element, the overflow can't be triggered, however the matroskaparse element has no size checks.
CVE-2022-2122	DOS / potential heap overwrite in qtdemux using zlib decompression. Integer overflow in qtdemux element in qtdemux_inflate function which causes a segfault, or could cause a heap overwrite, depending on libc and OS. Depending on the libc used, and the underlying OS capabilities, it could be just a segfault or a heap overwrite.
CVE-2022-26113	An execution with unnecessary privileges vulnerability [CWE-250] in FortiClientWindows 7.0.0 through 7.0.3, 6.4.0 through 6.4.7, 6.2.0 through 6.2.9, 6.0.0 through 6.0.10 may allow a local attacker to perform an arbitrary file write on the system.
CVE-2022-21524	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 network access via SMB 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 as well as unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized read access to a subset of Oracle Solaris accessible data. 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:L/I:L/A:H).
CVE-2022-30621	Allows a remote user to read files on the camera's OS "GetFileContent.cgi". Reading arbitrary files on the camera's OS as root user.
CVE-2022-34761	A CWE-476: NULL Pointer Dereference vulnerability exists that could cause a denial of service of the webserver when parsing JSON content type. Affected Products: X80 advanced RTU Communication Module (BMENOR2200H) (V2.01 and later), OPC UA Modicon Communication Module (BMENUA0100) (V1.10 and prior)
CVE-2022-21570	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 3.7.1.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Coherence. 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).
CVE-2022-20234	In Car Settings app, the NotificationAccessConfirmationActivity is exported. In NotificationAccessConfirmationActivity, it gets both 'mComponentName' and 'pkgTitle' from user.An unprivileged app can use a malicous mComponentName with a benign pkgTitle (e.g. Settings app) to make users enable notification access permission for the malicious app. That is, users believe they enable the notification access permission for the Settings app, but actually they enable the notification access permission for the malicious app.Once the malicious app gets the notification access permission, it can read all notifications, including users' personal information.Product: AndroidVersions: Android-12LAndroid ID: A-225189301
CVE-2022-20236	A drm driver have oob problem, could cause the system crash or EOPProduct: AndroidVersions: Android SoCAndroid ID: A-233124709
CVE-2022-22982	The vCenter Server contains a server-side request forgery (SSRF) vulnerability. A malicious actor with network access to 443 on the vCenter Server may exploit this issue by accessing a URL request outside of vCenter Server or accessing an internal service.

CVE Number	Description
CVE-2022-21567	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Worklist). 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 Workflow. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Workflow 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).
CVE-2022-32387	In Kentico before 13.0.66, attackers can achieve Denial of Service via a crafted request to the GetResource handler.
CVE-2022-21566	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.2.9-12.2.11. Easily exploitable vulnerability allows unauthenticated 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 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).
CVE-2022-34760	A CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability exists that could cause a denial of service of the webserver due to improper handling of the cookies. Affected Products: X80 advanced RTU Communication Module (BMENOR2200H) (V1.0), OPC UA Modicon Communication Module (BMENUA0100) (V1.10 and prior)
CVE-2021-24655	The WP User Manager WordPress plugin before 2.6.3 does not ensure that the user ID to reset the password of is related to the reset key given. As a result, any authenticated user can reset the password (to an arbitrary value) of any user knowing only their ID, and gain access to their account.
CVE-2022-34534	Digital Watchdog DW Spectrum Server 4.2.0.32842 allows attackers to access sensitive infromation via a crafted API call.
CVE-2022-21562	Vulnerability in the Oracle SOA Suite product of Oracle Fusion Middleware (component: Fabric Layer). 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).
CVE-2022-26655	Pexip Infinity 27.x before 27.3 has Improper Input Validation. The client API allows remote attackers to trigger a software abort via a gateway call into Teams.
CVE-2021-34538	Apache Hive before 3.1.3 "CREATE" and "DROP" function operations does not check for necessary authorization of involved entities in the query. It was found that an unauthorized user can manipulate an existing UDF without having the privileges to do so. This allowed unauthorized or underprivileged users to drop and recreate UDFs pointing them to new jars that could be potentially malicious.
CVE-2022-34027	Nginx NJS v0.7.4 was discovered to contain a segmentation violation via njs_value_property at njs_value.c.
CVE-2022-34028	Nginx NJS v0.7.5 was discovered to contain a segmentation violation via njs_utf8_next at src/njs_utf8.h.
CVE-2022-34030	Nginx NJS v0.7.5 was discovered to contain a segmentation violation via njs_djb_hash at src/njs_djb_hash.c.
CVE-2022-34031	Nginx NJS v0.7.5 was discovered to contain a segmentation violation via njs_value_to_number at src/njs_value_conversion.h.
CVE-2022-34032	Nginx NJS v0.7.5 was discovered to contain a segmentation violation in the function njs_value_own_enumerate at src/njs_value.c.
CVE-2022-34033	HTMLDoc v1.9.15 was discovered to contain a heap overflow via (write_header) /htmldoc/htmldoc/html.cxx:273.
CVE-2022-34035	HTMLDoc v1.9.12 and below was discovered to contain a heap overflow via e_node htmldoc/htmldoc/html.cxx:588.
CVE-2022-26654	Pexip Infinity before 27.3 allows remote attackers to force a software abort via HTTP.
CVE-2022-27928	Pexip Infinity 27.x before 27.3 allows remote attackers to trigger a software abort via the Session Initiation Protocol.

CVE Number	Description
CVE-2022-26657	Pexip Infinity before 27.3 allows remote attackers to trigger a software abort via One Touch Join.
CVE-2022-30634	Infinite loop in Read in crypto/rand before Go 1.17.11 and Go 1.18.3 on Windows allows attacker to cause an indefinite hang by passing a buffer larger than 1 << 32 - 1 bytes.
CVE-2022-36127	A vulnerability in Apache SkyWalking NodeJS Agent prior to 0.5.1. The vulnerability will cause NodeJS services that has this agent installed to be unavailable if the OAP is unhealthy and NodeJS agent can't establish the connection.
CVE-2022-32096	Rhonabwy before v1.1.5 was discovered to contain a buffer overflow via the component r_jwe_aesgcm_key_unwrap. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted JWE token.
CVE-2020-16093	In LemonLDAP::NG (aka lemonldap-ng) through 2.0.8, validity of the X.509 certificate is not checked by default when connecting to remote LDAP backends, because the default configuration of the Net::LDAPS module for Perl is used.
CVE-2022-33903	Tor 0.4.7.x before 0.4.7.8 allows a denial of service via the wedging of RTT estimation.
CVE-2022-31213	An issue was discovered in dbus-broker before 31. Multiple NULL pointer dereferences can be found when supplying a malformed XML config file.
CVE-2022-31212	An issue was discovered in dbus-broker before 31. It depends on c-uitl/c-shquote to parse the DBus service's Exec line. c-shquote contains a stack-based buffer over-read if a malicious Exec line is supplied.
CVE-2022-31781	Apache Tapestry up to version 5.8.1 is vulnerable to Regular Expression Denial of Service (ReDoS) in the way it handles Content Types. Specially crafted Content Types may cause catastrophic backtracking, taking exponential time to complete. Specifically, this is about the regular expression used on the parameter of the org.apache.tapestry5.http.ContentType class. Apache Tapestry 5.8.2 has a fix for this vulnerability. Notice the vulnerability cannot be triggered by web requests in Tapestry code alone. It would only happen if there's some non-Tapestry codepath passing some outside input to the ContentType class constructor.
CVE-2022-32389	Isode SWIFT v4.0.2 was discovered to contain hard-coded credentials in the Registry Editor. This allows attackers to access sensitive information such as user credentials and certificates.
CVE-2021-40150	The web server of the E1 Zoom camera through 3.0.0.716 discloses its configuration via the /conf/ directory that is mapped to a publicly accessible path. In this way an attacker can download the entire NGINX/FastCGI configurations by querying the /conf/nginx.conf or /conf/fastcgi.conf URI.
CVE-2022-32263	Pexip Infinity before 28.1 allows remote attackers to trigger a software abort via G.719.
CVE-2022-29286	Pexip Infinity 27 before 28.0 allows remote attackers to trigger excessive resource consumption and termination because of registrar resource mishandling.
CVE-2022-34169	The Apache Xalan Java XSLT library is vulnerable to an integer truncation issue when processing malicious XSLT stylesheets. This can be used to corrupt Java class files generated by the internal XSLTC compiler and execute arbitrary Java bytecode. Users are recommended to update to version 2.7.3 or later. Note: Java runtimes (such as OpenJDK) include repackaged copies of Xalan.
CVE-2022-27937	Pexip Infinity before 27.3 allows remote attackers to trigger excessive resource consumption via H.264.
CVE-2022-27936	Pexip Infinity before 27.3 allows remote attackers to trigger a software abort via H.323.
CVE-2022-27935	Pexip Infinity before 27.3 allows remote attackers to trigger a software abort via Epic Telehealth.
CVE-2022-27934	Pexip Infinity before 27.3 allows remote attackers to trigger a software abort via HTTP.
CVE-2022-20224	In AT_SKIP_REST of bta_hf_client_at.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure in the Bluetooth stack with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-220732646

CVE Number	Description
CVE-2022-27932	Pexip Infinity before 27.3 allows remote attackers to trigger a software abort via One Touch Join.
CVE-2022-27931	Pexip Infinity before 27.3 allows remote attackers to trigger a software abort via the Session Initiation Protocol.
CVE-2022-23745	A potential memory corruption issue was found in Capsule Workspace Android app (running on GrapheneOS). This could result in application crashing but could not be used to gather any sensitive information.
CVE-2022-27929	Pexip Infinity 27.x before 27.3 allows remote attackers to trigger a software abort via HTTP.
CVE-2022-28370	On Verizon 5G Home LVSKIHP OutDoorUnit (ODU) 3.33.101.0 devices, the RPC endpoint crtc_fw_upgrade provides a means of provisioning a firmware update for the device. /lib/functions/wnc_jsonsh/wnc_crtc_fw.sh has no cryptographic validation of the image, thus allowing an attacker to modify the installed firmware.
CVE-2022-34759	A CWE-787: Out-of-bounds Write vulnerability exists that could cause a denial of service of the webserver due to improper parsing of the HTTP Headers. Affected Products: X80 advanced RTU Communication Module (BMENOR2200H) (V1.0), OPC UA Modicon Communication Module (BMENUA0100) (V1.10 and prior)
CVE-2022-25891	The package github.com/containrrr/shoutrrr/pkg/util before 0.6.0 are vulnerable to Denial of Service (DoS) via the util.PartitionMessage function. Exploiting this vulnerability is possible by sending exactly 2000, 4000, or 6000 characters messages.
CVE-2022-21514	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Remote Administration Daemon). The supported version that is affected is 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols 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 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).
CVE-2022-32298	Toybox v0.8.7 was discovered to contain a NULL pointer dereference via the component httpd.c. This vulnerability can lead to a Denial of Service (DoS) via unspecified vectors.
CVE-2022-32297	Piwigo v12.2.0 was discovered to contain SQL injection vulnerability via the Search function.
CVE-2022-31147	The jQuery Validation Plugin (jquery-validation) provides drop-in validation for forms. Versions of jquery-validation prior to 1.19.5 are vulnerable to regular expression denial of service (ReDoS) when an attacker is able to supply arbitrary input to the url2 method. This is due to an incomplete fix for CVE-2021-43306. Users should upgrade to version 1.19.5 to receive a patch.
CVE-2022-23141	ZXMP M721 has an information leak vulnerability. Since the serial port authentication on the ZBOOT interface is not effective although it is enabled, an attacker could use this vulnerability to log in to the device to obtain sensitive information.
CVE-2022-34535	Digital Watchdog DW MEGApix IP cameras A7.2.2_20211029 allows unauthenticated attackers to view internal paths and scripts via web files.
CVE-2022-34536	Digital Watchdog DW MEGApix IP cameras A7.2.2_20211029 allows attackers to access the core log file and perform session hijacking via a crafted session token.
CVE-2022-31142	@fastify/bearer-auth is a Fastify plugin to require bearer Authorization headers. @fastify/bearer-auth prior to versions 7.0.2 and 8.0.1 does not securely use crypto.timingSafeEqual. A malicious attacker could estimate the length of one valid bearer token. According to the corresponding RFC 6750, the bearer token has only base64 valid characters, reducing the range of characters for a brute force attack. Version 7.0.2 and 8.0.1 of @fastify/bearer-auth contain a patch. There are currently no known workarounds. The package fastify-bearer-auth, which covers versions 6.0.3 and prior, is also vulnerable starting at version 5.0.1. Users of fastify-bearer-auth should upgrade to a patched version of @fastify/bearer-auth.
CVE-2022-22460	IBM Security Verify Identity Manager 10.0 contains sensitive information in the source code repository that could be used in further attacks against the system. IBM X-Force ID: 225013.
CVE-2022-22453	IBM Security Verify Identity Manager 10.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 224919.
CVE-2022-22452	IBM Security Verify Identity Manager 10.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 224918.
CVE-2022-2193	Insecure Direct Object Reference vulnerability in HYPR Server before version 6.14.1 allows remote authenticated attackers to add a FIDO2 authenticator to arbitrary accounts via parameter tampering in the Device Manager page. This issue affects: HYPR Server versions prior to 6.14.1.

CVE Number	Description
CVE-2022-28371	On Verizon 5G Home LVSKIHP InDoorUnit (IDU) 3.4.66.162 and OutDoorUnit (ODU) 3.33.101.0 devices, the CRTC and ODU RPC endpoints rely on a static certificate for access control. This certificate is embedded in the firmware, and is identical across the fleet of devices. An attacker need only download this firmware and extract the private components of these certificates (from /etc/lighttpd.d/ca.pem and /etc/lighttpd.d/server.pem) to gain access. (The firmware download location is shown in a device's upgrade logs.)
CVE-2022-2192	Forced Browsing vulnerability in HYPR Server version 6.10 to 6.15.1 allows remote attackers with a valid one-time recovery token to elevate privileges via path tampering in the Magic Link page. This issue affects: HYPR Server versions later than 6.10; version 6.15.1 and prior versions.
CVE-2022-31158	LTI 1.3 Tool Library is a library used for building IMS-certified LTI 1.3 tool providers in PHP. Prior to version 5.0, the Nonce Claim Value was not being validated against the nonce value sent in the Authentication Request. Users should upgrade to version 5.0 to receive a patch. There are currently no known workarounds.
CVE-2020-14127	A denial of service vulnerability exists in some Xiaomi models of phones. The vulnerability is caused by heap overflow and can be exploited by attackers to make remote denial of service.
CVE-2022-28377	On Verizon 5G Home LVSKIHP InDoorUnit (IDU) 3.4.66.162 and OutDoorUnit (ODU) 3.33.101.0 devices, the CRTC and ODU RPC endpoints rely on a static account username/password for access control. This password can be generated via a binary included in the firmware, after ascertaining the MAC address of the IDU's base Ethernet interface, and adding the string DEVICE_MANUFACTURER='Wistron_NeWeb_Corp.' to /etc/device_info to replicate the host environment. This occurs in /etc/init.d/wnc_factoryssidkeypwd (IDU).
CVE-2022-28372	On Verizon 5G Home LVSKIHP InDoorUnit (IDU) 3.4.66.162 and OutDoorUnit (ODU) 3.33.101.0 devices, the CRTC and ODU RPC endpoints provide a means of provisioning a firmware update for the device via crtc_fw_upgrade or crtcfwimage. The URL provided is not validated, and thus allows for arbitrary file upload to the device. This occurs in /lib/lua/luci/crtc.lua (IDU) and /lib/functions/wnc_jsonsh/wnc_crtc_fw.sh (ODU).
CVE-2022-31157	LTI 1.3 Tool Library is a library used for building IMS-certified LTI 1.3 tool providers in PHP. Prior to version 5.0, the function used to generate random nonces was not sufficiently cryptographically complex. Users should upgrade to version 5.0 to receive a patch. There are currently no known workarounds.
CVE-2022-21542	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime). Supported versions that are affected are 9.2.6.3 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. 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 and unauthorized ability to cause a partial denial of service (partial DOS) of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L).
CVE-2022-21516	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Enterprise Manager Install). 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 update, insert or delete access to some of Enterprise Manager Base Platform accessible data as well as unauthorized read access to a subset of Enterprise Manager Base Platform accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Enterprise Manager Base Platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).
CVE-2022-32223	Node.js is vulnerable to Hijack Execution Flow: DLL Hijacking under certain conditions on Windows platforms.This vulnerability can be exploited if the victim has the following dependencies on a Windows machine:* OpenSSL has been installed and “C:\Program Files\Common Files\SSL\openssl.cnf” exists.Whenever the above conditions are present, `node.exe` will search for `providers.dll` in the current user directory.After that, `node.exe` will try to search for `providers.dll` by the DLL Search Order in Windows.It is possible for an attacker to place the malicious file `providers.dll` under a variety of paths and exploit this vulnerability.
CVE-2022-31097	Grafana is an open-source platform for monitoring and observability. Versions on the 8.x and 9.x branch prior to 9.0.3, 8.5.9, 8.4.10, and 8.3.10 are vulnerable to stored cross-site scripting via the Unified Alerting feature of Grafana. An attacker can exploit this vulnerability to escalate privilege from editor to admin by tricking an authenticated admin to click on a link. Versions 9.0.3, 8.5.9, 8.4.10, and 8.3.10 contain a patch. As a workaround, it is possible to disable alerting or use legacy alerting.
CVE-2017-20128	A vulnerability has been found in KB Messages PHP Script 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument username/password with the input 'or''=' leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20127	A vulnerability was found in KB Login Authentication Script 1.1 and classified as critical. Affected by this issue is some unknown functionality. The manipulation of the argument username/password with the input 'or''=' leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20126	A vulnerability was found in KB Affiliate Referral Script 1.0. It has been classified as critical. This affects an unknown part of the file /index.php. The manipulation of the argument username/password with the input 'or''=' leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-32323	AutoTrace v0.40.0 was discovered to contain a heap overflow via the ReadImage function at input-bmp.c:660.
CVE-2021-42923	ShowMyPC 3606 on Windows suffers from a DLL hijack vulnerability. If an attacker overwrites the file %temp%\ShowMyPC\-ShowMyPC3606\wodVPN.dll, it will run any malicious code contained in that file. The code will run with normal user privileges unless the user specifically runs ShowMyPC as administrator.

CVE Number	Description
CVE-2022-2467	A vulnerability has been found in SourceCodester Garage Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /login.php. The manipulation of the argument username with the input 1@a.com' AND (SELECT 6427 FROM (SELECT(SLEEP(5)))LwLu) AND 'hsvT'='hsvT leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20133	A vulnerability, which was classified as critical, was found in Itech Job Portal Script 9.13. This affects an unknown part of the file /admin. The manipulation leads to improper authentication. It is possible to initiate the attack remotely.
CVE-2022-1565	The plugin WP All Import is vulnerable to arbitrary file uploads due to missing file type validation via the wp_all_import_get_gz.php file in versions up to, and including, 3.6.7. This makes it possible for authenticated attackers, with administrator level permissions and above, to upload arbitrary files on the affected sites server which may make remote code execution possible.
CVE-2022-36126	An issue was discovered in Inductive Automation Ignition before 7.9.20 and 8.x before 8.1.17. The ScriptInvoke function allows remote attackers to execute arbitrary code by supplying a Python script.
CVE-2022-21552	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Search). 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 WebCenter Content. While the vulnerability is in Oracle WebCenter Content, 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 WebCenter Content accessible data as well as unauthorized read access to a subset of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).
CVE-2022-26482	An issue was discovered in Poly EagleEye Director II before 2.2.2.1. os.system command injection can be achieved by an admin.
CVE-2022-21511	Vulnerability in the Oracle Database - Enterprise Edition Recovery component of Oracle Database Server. For supported versions that are affected see note. Easily exploitable vulnerability allows high privileged attacker having EXECUTE ON DBMS_IR.EXECUTESQLSCRIPT privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Recovery. Successful attacks of this vulnerability can result in takeover of Oracle Database - Enterprise Edition Recovery. Note: None of the supported versions are affected. 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).
CVE-2022-34024	Barangay Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via the resident module editing function at /bmis/pages/resident/resident.php.
CVE-2022-32416	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/classes/Master.php?f=delete_product.
CVE-2022-27483	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiManager version 7.0.0 through 7.0.3, 6.4.0 through 6.4.7, 6.2.x and 6.0.x and FortiAnalyzer version 7.0.0 through 7.0.3, version 6.4.0 through 6.4.7, 6.2.x and 6.0.x allows attacker to execute arbitrary shell code as `root` user via `diagnose system` CLI commands.
CVE-2022-32450	AnyDesk 7.0.9 allows a local user to gain SYSTEM privileges via a symbolic link because the user can write to their own %APPDATA% folder (used for ad.trace and chat) but the product runs as SYSTEM when writing chat-room data there.
CVE-2022-22358	IBM Sterling Partner Engagement Manager 6.1.2, 6.2, and Cloud/SasS 22.2 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 220651.
CVE-2022-24691	An issue was discovered in DSK DSKNet 2.16.136.0 and 2.17.136.5. A SQL Injection vulnerability allows authenticated users to taint database data and extract sensitive information via crafted HTTP requests. The type of SQL Injection is blind boolean based.
CVE-2022-31107	Grafana is an open-source platform for monitoring and observability. In versions 5.3 until 9.0.3, 8.5.9, 8.4.10, and 8.3.10, it is possible for a malicious user who has authorization to log into a Grafana instance via a configured OAuth IdP which provides a login name to take over the account of another user in that Grafana instance. This can occur when the malicious user is authorized to log in to Grafana via OAuth, the malicious user's external user id is not already associated with an account in Grafana, the malicious user's email address is not already associated with an account in Grafana, and the malicious user knows the Grafana username of the target user. If these conditions are met, the malicious user can set their username in the OAuth provider to that of the target user, then go through the OAuth flow to log in to Grafana. Due to the way that external and internal user accounts are linked together during login, if the conditions above are all met then the malicious user will be able to log in to the target user's Grafana account. Versions 9.0.3, 8.5.9, 8.4.10, and 8.3.10 contain a patch for this issue. As a workaround, concerned users can disable OAuth login to their Grafana instance, or ensure that all users authorized to log in via OAuth have a corresponding user account in Grafana linked to their email address.
CVE-2022-21544	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.1-12.4, 14.0-14.3 and 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H).
CVE-2022-31144	Redis is an in-memory database that persists on disk. A specially crafted `XAUTOCLAIM` command on a stream key in a specific state may result with heap overflow, and potentially remote code execution. This problem affects versions on the 7.x branch prior to 7.0.4. The patch is released in version 7.0.4.

CVE Number	Description
CVE-2022-34754	A CWE-269: Improper Privilege Management vulnerability exists that could allow elevated functionality when guessing credentials. Affected Products: Acti9 PowerTag Link C (A9XELC10-A) (V1.7.5 and prior), Acti9 PowerTag Link C (A9XELC10-B) (V2.12.0 and prior)
CVE-2021-33656	When setting font with malicous data by ioctl cmd PIO_FONT,kernel will write memory out of bounds.
CVE-2022-30624	Browsing the admin.html page allows the user to reset the admin password. Also appears in the JS code for the password.
CVE-2022-30242	Honeywell Alerton Ascent Control Module (ACM) through 2022-05-04 allows unauthenticated configuration changes from remote users. This enables configuration data to be stored on the controller and then implemented. A user with malicious intent can send a crafted packet to change the controller configuration without the knowledge of other users, altering the controller's function capabilities. The changed configuration is not updated in the User Interface, which creates an inconsistency between the configuration display and the actual configuration on the controller. After the configuration change, remediation requires reverting to the correct configuration, requiring either physical or remote access depending on the configuration that was altered.
CVE-2022-21551	Vulnerability in Oracle GoldenGate (component: Oracle GoldenGate). The supported version that is affected is 21c: prior to 21.7.0.0.0; 19c: prior to 19.1.0.0.220719. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle GoldenGate. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle GoldenGate. CVSS 3.1 Base Score 6.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H).
CVE-2022-26118	A privilege chaining vulnerability [CWE-268] in FortiManager and FortiAnalyzer 6.0.x, 6.2.x, 6.4.0 through 6.4.7, 7.0.0 through 7.0.3 may allow a local and authenticated attacker with a restricted shell to escalate their privileges to root due to incorrect permissions of some folders and executable files on the system.
CVE-2022-21428	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.1-12.4, 14.0-14.3 and 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:L).
CVE-2022-34757	A CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists where weak cipher suites can be used for the SSH connection between Easergy Pro software and the device, which may allow an attacker to observe protected communication details. Affected Products: Easergy P5 (V01.401.102 and prior)
CVE-2022-21582	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Trade Finance accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Trade Finance accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Trade Finance. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:L).
CVE-2022-21578	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.1-12.4, 14.0-14.3 and 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:L).
CVE-2021-44170	A stack-based buffer overflow vulnerability [CWE-121] in the command line interpreter of FortiOS before 7.0.4 and FortiProxy before 2.0.8 may allow an authenticated attacker to execute unauthorized code or commands via specially crafted command line arguments.
CVE-2021-33655	When sending malicous data to kernel by ioctl cmd FBIOPUT_VSCREENINFO,kernel will write memory out of bounds.
CVE-2022-21585	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Trade Finance accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Trade Finance accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Trade Finance. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:L).

CVE Number	Description
CVE-2022-31156	Gradle is a build tool. Dependency verification is a security feature in Gradle Build Tool that was introduced to allow validation of external dependencies either through their checksum or cryptographic signatures. In versions 6.2 through 7.4.2, there are some cases in which Gradle may skip that verification and accept a dependency that would otherwise fail the build as an untrusted external artifact. This can occur in two ways. When signature verification is disabled but the verification metadata contains entries for dependencies that only have a `gpg` element but no `checksum` element. When signature verification is enabled, the verification metadata contains entries for dependencies with a `gpg` element but there is no signature file on the remote repository. In both cases, the verification will accept the dependency, skipping signature verification and not complaining that the dependency has no checksum entry. For builds that are vulnerable, there are two risks. Gradle could download a malicious binary from a repository outside your organization due to name squatting. For those still using HTTP only and not HTTPS for downloading dependencies, the build could download a malicious library instead of the expected one. Gradle 7.5 patches this issue by making sure to run checksum verification if signature verification cannot be completed, whatever the reason. Two workarounds are available: Remove all `gpg` elements from dependency verification metadata if you disable signature validation and/or avoid adding `gpg` entries for dependencies that do not have signature files.
CVE-2022-21565	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 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 creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).
CVE-2022-20217	There is a unauthorized broadcast in the SprdContactsProvider. A third-party app could use this issue to delete Fdn contact.Product: AndroidVersions: Android SoCAndroid ID: A-232441378
CVE-2022-31202	The export function in SoftGuard Web (SGW) before 5.1.5 allows directory traversal to read an arbitrary local file via export or man.tcl.
CVE-2019-10800	This affects the package codecov before 2.0.16. The vulnerability occurs due to not sanitizing gcov arguments before being being provided to the popen method.
CVE-2022-22359	IBM Sterling Partner Engagement Manager 6.1.2, 6.2, and Cloud/SasS 22.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 220652.
CVE-2022-21561	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime). Supported versions that are affected are 9.2.6.3 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Tools 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).
CVE-2022-32213	The llhttp parser <v14.20.1, <v16.17.1 and <v18.9.1 in the http module in Node.js does not correctly parse and validate Transfer-Encoding headers and can lead to HTTP Request Smuggling (HRS).
CVE-2022-32210	`Undici.ProxyAgent` never verifies the remote server's certificate, and always exposes all request & response data to the proxy. This unexpectedly means that proxies can MitM all HTTPS traffic, and if the proxy's URL is HTTP then it also means that nominally HTTPS requests are actually sent via plain-text HTTP between Undici and the proxy server.
CVE-2022-21518	Vulnerability in the Oracle Health Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: User Interface). Supported versions that are affected are 2.4.8.7 and 2.5.2.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Data Management Workbench 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).
CVE-2022-30245	Honeywell Alerton Compass Software 1.6.5 allows unauthenticated configuration changes from remote users. This enables configuration data to be stored on the controller and then implemented. A user with malicious intent can send a crafted packet to change the controller configuration without the knowledge of other users, altering the controller's function capabilities. The changed configuration is not updated in the User Interface, which creates an inconsistency between the configuration display and the actual configuration on the controller. After the configuration change, remediation requires reverting to the correct configuration, requiring either physical or remote access depending on the configuration that was altered.
CVE-2022-20228	In various functions of C2DmaBufAllocator.cpp, there is a possible memory corruption due to a use after free. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-213850092
CVE-2022-30570	The Column Based Security component of TIBCO Software Inc.'s TIBCO Data Virtualization and TIBCO Data Virtualization for AWS Marketplace contains an easily exploitable vulnerability that allows a low privileged attacker with network access to obtain read access to application information on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Data Virtualization: versions 8.5.2 and below and TIBCO Data Virtualization for AWS Marketplace: versions 8.5.2 and below.
CVE-2022-2030	A directory traversal vulnerability caused by specific character sequences within an improperly sanitized URL was identified in some CGI programs of Zyxel USG FLEX 100(W) firmware versions 4.50 through 5.30, USG FLEX 200 firmware versions 4.50 through 5.30, USG FLEX 500 firmware versions 4.50 through 5.30, USG FLEX 700 firmware versions 4.50 through 5.30, USG FLEX 50(W) firmware versions 4.16 through 5.30, USG20(W)-VPN firmware versions 4.16 through 5.30, ATP series firmware versions 4.32 through 5.30, VPN series firmware versions 4.30 through 5.30, USG/ZyWALL series firmware versions 4.11 through 4.72, that could allow an authenticated attacker to access some restricted files on a vulnerable device.
CVE-2022-21569	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 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).

CVE Number	Description
CVE-2022-31153	OpenZeppelin Contracts for Cairo is a library for contract development written in Cairo for StarkNet, a decentralized ZK Rollup. Version 0.2.0 is vulnerable to an error that renders account contracts unusable on live networks. This issue affects all accounts (vanilla and ethereum flavors) in the v0.2.0 release of OpenZeppelin Contracts for Cairo, which are not whitelisted on StarkNet mainnet. Only goerli deployments of v0.2.0 accounts are affected. This faulty behavior is not observed in StarkNet's testing framework. This bug has been patched in v0.2.1.
CVE-2022-21568	Vulnerability in the Oracle iReceivables product of Oracle E-Business Suite (component: Access Request). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iReceivables. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iReceivables 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).
CVE-2022-31260	In Montala ResourceSpace through 9.8 before r19636, csv_export_results_metadata.php allows attackers to export collection metadata via a non-NULL k value.
CVE-2022-34001	Unit4 ERP through 7.9 allows XXE via ExecuteServerProcessAsynchronously.
CVE-2021-39017	IBM Engineering Lifecycle Optimization - Publishing 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 could allow a remote attacker to upload arbitrary files, caused by improper access controls. IBM X-Force ID: 213725.
CVE-2022-30302	Multiple relative path traversal vulnerabilities [CWE-23] in FortiDeceptor management interface 1.0.0 through 3.2.x, 3.3.0 through 3.3.2, 4.0.0 through 4.0.1 may allow a remote and authenticated attacker to retrieve and delete arbitrary files from the underlying filesystem via specially crafted web requests.
CVE-2022-21573	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Billing Care). Supported versions that are affected are 12.0.0.4.0-12.0.0.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Communications Billing and Revenue Management. 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).
CVE-2021-39019	IBM Engineering Lifecycle Optimization - Publishing 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 could disclose highly sensitive information through an HTTP GET request to an authenticated user. IBM X-Force ID: 213728.
CVE-2022-35283	IBM Security Verify Information Queue 10.0.2 could allow an authenticated user to cause a denial of service with a specially crafted HTTP request.
CVE-2022-21548	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).
CVE-2022-2108	The plugin Wbcom Designs – BuddyPress Group Reviews for WordPress is vulnerable to unauthorized settings changes and review modification due to missing capability checks and improper nonce checks in several functions related to said actions in versions up to, and including, 2.8.3. This makes it possible for unauthenticated attackers to modify reviews and plugin settings on the affected site.
CVE-2022-31145	FlyteAdmin is the control plane for Flyte responsible for managing entities and administering workflow executions. In versions 1.1.30 and prior, authenticated users using an external identity provider can continue to use Access Tokens and ID Tokens even after they expire. Users who use FlyteAdmin as the OAuth2 Authorization Server are unaffected by this issue. A patch is available on the `master` branch of the repository. As a workaround, rotating signing keys immediately will invalidate all open sessions and force all users to attempt to obtain new tokens. Those who use this workaround should continue to rotate keys until FlyteAdmin has been upgraded and hide FlyteAdmin deployment ingress URL from the internet.
CVE-2022-21556	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 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).
CVE-2022-2401	Unrestricted information disclosure of all users in Mattermost version 6.7.0 and earlier allows team members to access some sensitive information by directly accessing the APIs.
CVE-2022-32215	The llhttp parser <v14.20.1, <v16.17.1 and <v18.9.1 in the http module in Node.js does not correctly handle multi-line Transfer-Encoding headers. This can lead to HTTP Request Smuggling (HRS).
CVE-2021-46784	In Squid 3.x through 3.5.28, 4.x through 4.17, and 5.x before 5.6, due to improper buffer management, a Denial of Service can occur when processing long Gopher server responses.
CVE-2021-29799	IBM Engineering Requirements Quality Assistant On-Premises (All versions) could allow an authenticated user to obtain sensitive information due to improper client side validation. IBM X-Force ID: 203738.

CVE Number	Description
CVE-2021-38868	IBM Engineering Requirements Quality Assistant On-Premises (All versions) is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force Id: 208310.
CVE-2022-23825	Aliases in the branch predictor may cause some AMD processors to predict the wrong branch type potentially leading to information disclosure.
CVE-2022-20221	In avrc_ctrl_pars_vendor_cmd of avrc_pars_ct.cc, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-205571133
CVE-2022-32214	The llhttp parser <v14.20.1, <v16.17.1 and <v18.9.1 in the http module in Node.js does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS).
CVE-2022-22445	An attacker that gains service access to the FSP (POWER9 only) or gains admin authority to a partition can compromise partition firmware.
CVE-2022-21577	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.1-12.4, 14.0-14.3 and 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N).
CVE-2021-22131	A improper validation of certificate with host mismatch in Fortinet FortiTokenAndroid version 5.0.3 and below, Fortinet FortiTokeniOS version 5.2.0 and below, Fortinet FortiTokenWinApp version 4.0.3 and below allows attacker to retrieve information disclosed via man-in-the-middle attacks.
CVE-2022-21579	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.1-12.4, 14.0-14.3 and 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N).
CVE-2022-21583	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Trade Finance accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Trade Finance accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Trade Finance. CVSS 3.1 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L).
CVE-2022-21584	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Trade Finance accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Trade Finance accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N).
CVE-2022-2101	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `file[files][]` parameter in versions up to, and including, 3.2.46 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor level permissions and above to inject arbitrary web scripts on the file's page that will execute whenever an administrator accesses the editor area for the injected file page.
CVE-2022-21576	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L).
CVE-2022-21586	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Trade Finance accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Trade Finance accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N).
CVE-2017-20132	A vulnerability was found in Itech Multi Vendor Script 6.49 and classified as critical. This issue affects some unknown processing of the file /multi-vendor-shopping-script/product-list.php. The manipulation of the argument pl leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2016-15003	A vulnerability has been found in FileZilla Client 3.17.0.0 and classified as problematic. This vulnerability affects unknown code of the file C:\Program Files\FileZilla FTP Client\uninstall.exe of the component Installer. The manipulation leads to unquoted search path. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.

CVE Number	Description
CVE-2017-20131	A vulnerability was found in Itech News Portal 6.28. It has been classified as critical. Affected is an unknown function of the file /news-portal-script/information.php. The manipulation of the argument inf leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-30626	Browsing the path: http://ip/wifi_ap_pata_get.cmd, will show in the name of the existing access point on the component, and a password in clear text.
CVE-2017-20129	A vulnerability was found in LogoStore. It has been classified as critical. Affected is an unknown function of the file /LogoStore/search.php. The manipulation of the argument query with the input test' UNION ALL SELECT CONCAT(CONCAT('qqkkq','VnPVWVaYxljWqGpLLbEIyPIHBjjjjASQTnaqfKaV'),'qvvpq'),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- oCrh&search= leads to sql injection. It is possible to launch the attack remotely.
CVE-2022-2468	A vulnerability was found in SourceCodester Garage Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /editbrand.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.
CVE-2017-20130	A vulnerability was found in Itech Real Estate Script 3.12. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /real-estate-script/search_property.php. The manipulation of the argument property_for leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-21550	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.36 and prior, 7.5.26 and prior, 7.6.22 and prior and and 8.0.29 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).
CVE-2017-20138	A vulnerability was found in Itech Auction Script 6.49. It has been classified as critical. This affects an unknown part of the file /mcategory.php. The manipulation of the argument mcid with the input 4' AND 1734=1734 AND 'Ggks'='Ggks leads to sql injection (Blind). It is possible to initiate the attack remotely.
CVE-2017-20135	A vulnerability classified as critical was found in Itech Dating Script 3.26. Affected by this vulnerability is an unknown functionality of the file /see_more_details.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20137	A vulnerability was found in Itech B2B Script 4.28. It has been rated as critical. This issue affects some unknown processing of the file /catcompany.php. The manipulation of the argument token with the input 704667c6a1e7ce56d3d6fa748ab6d9af3fd7' AND 6539=6539 AND 'Fakj'='Fakj leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20134	A vulnerability, which was classified as critical, has been found in Itech Freelancer Script 5.13. Affected by this issue is some unknown functionality of the file /category.php. The manipulation of the argument sk leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20136	A vulnerability classified as critical has been found in Itech Classifieds Script 7.27. Affected is an unknown function of the file /subpage.php. The manipulation of the argument scat with the input =51' AND 4941=4941 AND 'hoCP'='hoCP leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-1933	The CDI WordPress plugin before 5.1.9 does not sanitise and escape a parameter before outputting it back in the response of an AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting
CVE-2022-36303	Vesta v1.0.0-5 was discovered to contain a cross-site scripting (XSS) vulnerability via the handle_file_upload function at /web/api/v1/upload/UploadHandler.php.
CVE-2022-28681	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the deletePages method. By performing actions in JavaScript, an attacker can trigger a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-16825.
CVE-2022-34093	Portal do Software Publico Brasileiro i3geo v7.0.5 was discovered to contain a cross-site scripting (XSS) vulnerability via access_token.php.
CVE-2022-34094	Portal do Software Publico Brasileiro i3geo v7.0.5 was discovered to contain a cross-site scripting (XSS) vulnerability via request_token.php.
CVE-2022-36305	Vesta v1.0.0-5 was discovered to contain a cross-site scripting (XSS) vulnerability via the body function at /web/api/v1/upload/UploadHandler.php.
CVE-2022-36304	Vesta v1.0.0-5 was discovered to contain a cross-site scripting (XSS) vulnerability via the generate_response function at /web/api/v1/upload/UploadHandler.php.

CVE Number	Description
CVE-2022-2146	The Import CSV Files WordPress plugin through 1.0 does not sanitise and escaped imported data before outputting them back in a page, and is lacking CSRF check when performing such action as well, resulting in a Reflected Cross-Site Scripting
CVE-2022-34025	Vesta v1.0.0-5 was discovered to contain a cross-site scripting (XSS) vulnerability via the post function at /web/api/v1/upload/UploadHandler.php.
CVE-2022-2090	The Discount Rules for WooCommerce WordPress plugin before 2.4.2 does not escape a parameter before outputting it back in an attribute of the plugin's discount rule page, leading to Reflected Cross-Site Scripting
CVE-2022-29890	In affected versions of Octopus Server the help sidebar can be customized to include a Cross-Site Scripting payload in the support link.
CVE-2022-32118	Arox School ERP Pro v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the dispatchcategory parameter in backoffice.inc.php.
CVE-2020-35305	Cross site scripting (XSS) in gollum 5.0 to 5.1.2 via the filename parameter to the 'New Page' dialog.
CVE-2022-23201	Adobe RoboHelp versions 2020.0.7 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.
CVE-2022-2168	The Download Manager WordPress plugin before 3.2.44 does not escape a generated URL before outputting it back in an attribute of the history dashboard, leading to Reflected Cross-Site Scripting
CVE-2022-34092	Portal do Software Publico Brasileiro i3geo v7.0.5 was discovered to contain a cross-site scripting (XSS) vulnerability via svg2img.php.
CVE-2021-46827	An issue was discovered in Oxygen XML WebHelp before 22.1 build 2021082006 and 23.x before 23.1 build 2021090310. An XSS vulnerability in search terms proposals (in online documentation generated using Oxygen XML WebHelp) allows attackers to execute JavaScript by convincing a user to type specific text in the WebHelp output search field.
CVE-2022-22477	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 225605.
CVE-2022-21520	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Fluid Core). Supported versions that are affected are 8.58 and 8.59. 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).
CVE-2022-32308	Cross Site Scripting (XSS) vulnerability in uBlock Origin extension before 1.41.1 allows remote attackers to run arbitrary code via a spoofed 'MessageSender.url' to the browser renderer process.
CVE-2022-25802	Best Practical Request Tracker (RT) before 4.4.6 and 5.x before 5.0.3 allows XSS via a crafted content type for an attachment.
CVE-2022-22304	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiAuthenticator OWA Agent for Microsoft version 2.2 and 2.1 may allow an unauthenticated attacker to perform an XSS attack via crafted HTTP GET requests.
CVE-2022-25803	Best Practical Request Tracker (RT) before 5.0.3 has an Open Redirect via a ticket search.
CVE-2022-2187	The Contact Form 7 Captcha WordPress plugin before 0.1.2 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers
CVE-2022-32225	A reflected DOM-Based XSS vulnerability has been discovered in the Help directory of Veeam Management Pack for Microsoft System Center 8.0. This vulnerability could be exploited by an attacker by convincing a legitimate user to visit a crafted URL on a Veeam Management Pack for Microsoft System Center server, allowing for the execution of arbitrary scripts.
CVE-2022-2173	The Advanced Database Cleaner WordPress plugin before 3.1.1 does not escape numerous generated URLs before outputting them back in href attributes of admin dashboard pages, leading to Reflected Cross-Site Scripting

CVE Number	Description
CVE-2022-21575	Vulnerability in the Oracle WebCenter Sites Support Tools product of Oracle Fusion Middleware (component: User Interface). The supported version that is affected is Prior to 4.4.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites Support Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites Support Tools accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Sites Support Tools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Sites Support Tools. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:L).
CVE-2022-27930	Pexip Infinity 27.x before 27.3 allows remote attackers to trigger a software abort via single-sign-on if a random Universally Unique Identifier is guessed.
CVE-2022-21519	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.29 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Cluster. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2022-34826	In Couchbase Server 7.1.x before 7.1.1, an encrypted Private Key passphrase may be leaked in the logs.
CVE-2021-40149	The web server of the E1 Zoom camera through 3.0.0.716 discloses its SSL private key via the root web server directory. In this way an attacker can download the entire key via the /self.key URI.
CVE-2022-29593	relay_cgi.cgi on Dingtian DT-R002 2CH relay devices with firmware 3.1.276A allows an attacker to replay HTTP post requests without the need for authentication or a valid signed/authorized request.
CVE-2022-34764	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause denial of service when parsing the URL. Affected Products: X80 advanced RTU Communication Module (BMENOR2200H) (V1.0), OPC UA Modicon Communication Module (BMENUA0100) (V1.10 and prior)
CVE-2022-34763	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists that could cause loading of unauthorized firmware images due to improper verification of the firmware signature. Affected Products: X80 advanced RTU Communication Module (BMENOR2200H) (V2.01 and later), OPC UA Modicon Communication Module (BMENUA0100) (V1.10 and prior)
CVE-2022-34762	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause unauthorized firmware image loading when unsigned images are added to the firmware image path. Affected Products: X80 advanced RTU Communication Module (BMENOR2200H) (V2.01 and later), OPC UA Modicon Communication Module (BMENUA0100) (V1.10 and prior)
CVE-2022-21541	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. 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 creation, deletion or modification access to critical data or all 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 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2022-30623	The server checks the user's cookie in a non-standard way, and a value is entered in the cookie value name of the status and its value is set to true to bypass the identification with the system using a username and password.
CVE-2022-21580	Vulnerability in the Oracle Financial Services Revenue Management and Billing product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 2.9.0.0.0, 2.9.0.1.0, 3.0.0.0.0-3.2.0.0.0 and 4.0.0.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Revenue Management and Billing. 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 Financial Services Revenue Management and Billing accessible data as well as unauthorized update, insert or delete access to some of Oracle Financial Services Revenue Management and Billing accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Revenue Management and Billing. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L).
CVE-2022-21581	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Trade Finance. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:L).

CVE Number	Description
CVE-2022-21508	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.3. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Essbase executes to compromise Oracle Essbase. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Essbase accessible data as well as unauthorized access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 5.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N).
CVE-2022-2393	A flaw was found in pki-core, which could allow a user to get a certificate for another user identity when directory-based authentication is enabled. This flaw allows an authenticated attacker on the adjacent network to impersonate another user within the scope of the domain, but they would not be able to decrypt message content.
CVE-2022-21557	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 creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N).
CVE-2022-30627	This vulnerability affects all of the company's products that also include the FW versions: update_i90_cv2.021_b20210104, update_i50_v1.0.55_b20200509, update_x6_v2.1.2_b202001127, update_b5_v2.0.9_b20200706. This vulnerability makes it possible to extract from the FW the existing user passwords on their operating systems and passwords.
CVE-2022-30625	Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. A directory listing provides an attacker with the complete index of all the resources located inside of the directory. The specific risks and consequences vary depending on which files are listed and accessible.
CVE-2022-21527	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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2022-34232	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (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.
CVE-2022-34244	Adobe Photoshop versions 22.5.7 (and earlier) and 23.3.2 (and earlier) are affected by an Access of Uninitialized Pointer 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.
CVE-2022-34239	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (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.
CVE-2022-34237	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (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..
CVE-2022-34236	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (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.
CVE-2022-34234	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (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.
CVE-2021-4135	A memory leak vulnerability was found in the Linux kernel's eBPF for the Simulated networking device driver in the way user uses BPF for the device such that function nsim_map_alloc_elem being called. A local user could use this flaw to get unauthorized access to some data.
CVE-2022-20227	In USB driver, there is a possible out of bounds read due to a heap buffer overflow. 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-216825460References: Upstream kernel
CVE-2022-34233	Adobe Acrobat Reader versions 22.001.20142 (and earlier), 20.005.30334 (and earlier) and 17.012.30229 (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.
CVE-2022-32317	The MPlayer Project v1.5 was discovered to contain a heap use-after-free resulting in a double free in the preinit function at libvo/vo_v4l2.c. This vulnerability can lead to a Denial of Service (DoS) via a crafted file. The device=strdup statement is not executed on every call. Note: This has been disputed by third parties as invalid and not reproduceable.
CVE-2020-23563	IrfanView 4.54 allows a user-mode write access violation starting at FORMATS!ShowPlugInSaveOptions_W+0x0000000000002cba.

CVE Number	Description
CVE-2022-20230	In choosePrivateKeyAlias of KeyChain.java, there is a possible access to the user's certificate due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-221859869
CVE-2022-2380	The Linux kernel was found vulnerable out of bounds memory access in the drivers/video/fbdev/sm712fb.c:smtcfb_read() function. The vulnerability could result in local attackers being able to crash the kernel.
CVE-2022-34266	The libtiff-4.0.3-35.amzn2.0.1 package for LibTIFF on Amazon Linux 2 allows attackers to cause a denial of service (application crash), a different vulnerability than CVE-2022-0562. When processing a malicious TIFF file, an invalid range may be passed as an argument to the memset() function within TIFFFetchStripThing() in tif_dirread.c. This will cause TIFFFetchStripThing() to segfault after use of an uninitialized resource.
CVE-2022-2476	A null pointer dereference bug was found in wavpack-5.4.0 The results from the ASAN log: AddressSanitizer:DEADLYSIGNAL ===84257==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x561b47a970c6 bp 0x7fff13952fb0 sp 0x7fff1394fca0 T0) ==84257==The signal is caused by a WRITE memory access. ==84257==Hint: address points to the zero page. #0 0x561b47a970c5 in main cli/wvunpack.c:834 #1 0x7efc4f5c0082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082) #2 0x561b47a945ed in _start (/usr/local/bin/wvunpack+0xa5ed) AddressSanitizer can not provide additional info. SUMMARY: AddressSanitizer: SEGV cli/wvunpack.c:834 in main ==84257==ABORTING
CVE-2022-32406	GtkRadiant v1.6.6 was discovered to contain a buffer overflow via the component q3map2. This vulnerability can cause a Denial of Service (DoS) via a crafted MAP file.
CVE-2022-34765	A CWE-73: External Control of File Name or Path vulnerability exists that could cause loading of unauthorized firmware images when user-controlled data is written to the file path. Affected Products: X80 advanced RTU Communication Module (BMENOR2200H) (V2.01 and later), OPC UA Modicon Communication Module (BMENUA0100) (V1.10 and prior)
CVE-2020-23561	IrfanView 4.54 allows a user-mode write access violation starting at FORMATS!ShowPlugInSaveOptions_W+0x0000000000005722.
CVE-2020-23562	IrfanView 4.54 allows a user-mode write access violation starting at FORMATS!ShowPlugInSaveOptions_W+0x000000000000aefe.
CVE-2022-34248	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2022-34252	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (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.
CVE-2022-34634	CVA6 commit d315ddd0f1be27c1b3f27eb0b8daf471a952299a executes crafted or incorrectly formatted det instructions rather create an exception.
CVE-2022-34639	CVA6 commit d315ddd0f1be27c1b3f27eb0b8daf471a952299a treats non-standard fence instructions as illegal which can affect the function of the application.
CVE-2022-21528	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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2022-21533	Vulnerability in the Oracle Solaris product of Oracle Systems (component: SMB Server). 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).
CVE-2022-20219	In multiple functions of StorageManagerService.java and UserManagerService.java, there is a possible way to leave user's directories unencrypted due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-224585613
CVE-2022-21509	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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2022-34633	CVA6 commit d315ddd0f1be27c1b3f27eb0b8daf471a952299a executes crafted or incorrectly formatted sfence.vma instructions rather create an exception.

CVE Number	Description
CVE-2022-34636	CVA6 commit d315ddd0f1be27c1b3f27eb0b8daf471a952299a and RISCV-Boom commit ad64c5419151e5e886daee7084d8399713b46b4b implements the incorrect exception type when a PMA violation occurs during address translation.
CVE-2022-34637	CVA6 commit d315ddd0f1be27c1b3f27eb0b8daf471a952299a implements an incorrect exception type when an illegal virtual address is loaded.
CVE-2022-21559	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11.3.0, 11.3.1 and 11.3.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Commerce Platform executes to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Platform 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).
CVE-2022-34640	The *tval of ecall/ebreak in CVA6 commit d315ddd0f1be27c1b3f27eb0b8daf471a952299a was discovered to be incorrect.
CVE-2022-34641	CVA6 commit d315ddd0f1be27c1b3f27eb0b8daf471a952299a and RISCV-Boom commit ad64c5419151e5e886daee7084d8399713b46b4b implements the incorrect exception type when a PMP violation occurs during address translation.
CVE-2022-34642	The component mcontrol.action in RISCV ISA Sim commit ac466a21df442c59962589ba296c702631e041b5 contains the incorrect mask which can cause a Denial of Service (DoS).
CVE-2022-34643	RISCV ISA Sim commit ac466a21df442c59962589ba296c702631e041b5 implements the incorrect exception priotrity when accessing memory.
CVE-2022-1662	In convert2rhel, there's an ansible playbook named ansible/run-convert2rhel.yml which passes the Red Hat Subscription Manager user password via the CLI to convert2rhel. This could allow unauthorized local users to view the password via the process list while convert2rhel is running. However, this ansible playbook is only an example in the upstream repository and it is not shipped in officially supported versions of convert2rhel.
CVE-2022-20225	In getSubscriptionProperty of SubscriptionController.java, there is a possible read of a sensitive identifier due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-213457638
CVE-2022-30982	An issue was discovered in Gentics CMS before 5.43.1. There is stored XSS in the profile description and in the username.
CVE-2021-39015	IBM Engineering Lifecycle Optimization - Publishing 7.0, 7.0.1, and 7.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 213655.
CVE-2022-32318	Fast Food Ordering System v1.0 was discovered to contain a persistent cross-site scripting (XSS) vulnerability via the component /ffos/classes/Master.php?f=save_category.
CVE-2022-2224	The WordPress plugin Gallery for Social Photo is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.0.0.27 due to failure to properly check for the existence of a nonce in the function gifeed_duplicate_feed. This make it possible for unauthenticated attackers to duplicate existing posts or pages granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2022-34537	Digital Watchdog DW MEGApix IP cameras A7.2.2_20211029 was discovered to contain a cross-site scripting (XSS) vulnerability via the component bia_oneshot.cgi.
CVE-2021-29788	IBM Engineering Requirements Quality Assistant On-Premises (All versions) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 203310.
CVE-2021-29790	IBM Engineering Requirements Quality Assistant On-Premises (All versions) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 203440.
CVE-2022-2223	The WordPress plugin Image Slider is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.1.121 due to failure to properly check for the existence of a nonce in the function ewic_duplicate_slider. This make it possible for unauthenticated attackers to duplicate existing posts or pages granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2021-39028	IBM Engineering Lifecycle Optimization - Publishing 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 213866.
CVE-2022-31201	SoftGuard Web (SGW) before 5.1.5 allows HTML injection.

CVE Number	Description
CVE-2020-35261	Cross Site Scripting (XSS) vulnerability in sourcecodester Multi Restaurant Table Reservation System 1.0 via the Restaurant Name field to /dashboard/profile.php.
CVE-2020-36550	Cross Site Scripting (XSS) vulnerability in sourcecodester Multi Restaurant Table Reservation System 1.0 via the Table Name field to /dashboard/table-list.php.
CVE-2022-29057	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiEDR version 5.1.0, 5.0.0 through 5.0.3 Patch 6 and 4.0.0 allows a remote authenticated attacker to perform a reflected cross site scripting attack (XSS) by injecting malicious payload into the Management Console via various endpoints.
CVE-2022-34358	IBM i 7.2, 7.3, 7.4, and 7.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 230516.
CVE-2022-24692	An issue was discovered in DSK DSKNet 2.16.136.0 and 2.17.136.5. The new menu option within the general Parameters page is vulnerable to stored XSS. The attacker can create a menu option, make it visible to every application user, and conduct session hijacking, account takeover, or malicious code delivery, with the final goal of achieving client-side code execution.
CVE-2022-32074	A stored cross-site scripting (XSS) vulnerability in the component audit/class.audit.php of osTicket-plugins - Storage-FS before commit a7842d494889fd5533d13deb3c6a7789768795ae allows attackers to execute arbitrary web scripts or HTML via a crafted SVG file.
CVE-2022-26120	Multiple improper neutralization of special elements used in an SQL Command ('SQL Injection') vulnerabilities [CWE-89] in FortiADC management interface 7.0.0 through 7.0.1, 5.0.0 through 6.2.2 may allow an authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.
CVE-2022-32065	An arbitrary file upload vulnerability in the background management module of RuoYi v4.7.3 and below allows attackers to execute arbitrary code via a crafted HTML file.
CVE-2020-36553	Cross Site Scripting (XSS) vulnerability in sourcecodester Multi Restaurant Table Reservation System 1.0 via the Area(food_type) field to /dashboard/menu-list.php.
CVE-2022-22416	IBM Sterling Partner Engagement Manager 6.1.2, 6.2, and Cloud/SasS 22.2 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 223126.
CVE-2022-22417	IBM Sterling Partner Engagement Manager 6.1.2, 6.2, and Cloud/SasS 22.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 223127.
CVE-2020-36552	Cross Site Scripting (XSS) vulnerability in sourcecodester Multi Restaurant Table Reservation System 1.0 via the Made field to /dashboard/menu-list.php.
CVE-2020-36551	Cross Site Scripting (XSS) vulnerability in sourcecodester Multi Restaurant Table Reservation System 1.0 via the Item Name field to /dashboard/menu-list.php.
CVE-2022-32274	The Transition Scheduler add-on 6.5.0 for Atlassian Jira is prone to stored XSS via the project name to the creation function.
CVE-2022-21572	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Billing Care). Supported versions that are affected are 12.0.0.4.0-12.0.0.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Billing and Revenue Management, 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 Communications Billing and Revenue Management accessible data as well as unauthorized read access to a subset of Oracle Communications Billing and Revenue 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:R/S:C/C:L/I:L/A:N).
CVE-2022-21574	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.4.0-12.0.0.6.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Communications Billing and Revenue Management. 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).
CVE-2022-25357	Pexip Infinity 27.x before 27.2 has Improper Access Control. An attacker can sometimes join a conference (call join) if it has a lock but not a PIN.

CVE Number	Description
CVE-2022-21545	Vulnerability in the Oracle iRecruitment product of Oracle E-Business Suite (component: Candidate Self Service Registration). 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 iRecruitment. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iRecruitment 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).
CVE-2022-32222	A cryptographic vulnerability exists on Node.js on linux in versions of 18.x prior to 18.40.0 which allowed a default path for openssl.cnf that might be accessible under some circumstances to a non-admin user instead of /etc/ssl as was the case in versions prior to the upgrade to OpenSSL 3.
CVE-2022-2400	External Control of File Name or Path in GitHub repository dompdf/dompdf prior to 2.0.0.
CVE-2022-21540	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Easily exploitable 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 read access to a subset 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 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2022-22473	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to obtain sensitive information caused by improper handling of Administrative Console data. This information could be used in further attacks against the system. IBM X-Force ID: 225347.
CVE-2022-23142	ZXEN CG200 has a DoS vulnerability. An attacker could construct and send a large number of HTTP GET requests in a short time, which can make the product management websites not accessible.
CVE-2022-2117	The GiveWP plugin for WordPress is vulnerable to Sensitive Information Disclosure in versions up to, and including, 2.20.2 via the /donor-wall REST-API endpoint which provides unauthenticated users with donor information even when the donor wall is not enabled. This functionality has been completely removed in version 2.20.2.
CVE-2022-30532	In affected versions of Octopus Deploy, there is no logging of changes to artifacts within Octopus Deploy.
CVE-2022-31150	undici is an HTTP/1.1 client, written from scratch for Node.js. It is possible to inject CRLF sequences into request headers in undici in versions less than 5.7.1. A fix was released in version 5.8.0. Sanitizing all HTTP headers from untrusted sources to eliminate `\r\n` is a workaround for this issue.
CVE-2022-2133	The OAuth Single Sign On WordPress plugin before 6.22.6 doesn't validate that OAuth access token requests are legitimate, which allows attackers to log onto the site with the only knowledge of a user's email address.
CVE-2021-32504	Unauthenticated users can access sensitive web URLs through GET request, which should be restricted to maintenance users only. A malicious attacker could use this sensitive information’s to launch further attacks on the system.
CVE-2022-21560	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. 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).
CVE-2022-1881	In affected versions of Octopus Server an Insecure Direct Object Reference vulnerability exists where it is possible for a user to download Project Exports from a Project they do not have permissions to access. This vulnerability only impacts projects within the same Space.
CVE-2022-32425	The login function of Mealie v1.0.0beta-2 allows attackers to enumerate existing usernames by timing the server's response time.
CVE-2022-21564	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. 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).
CVE-2022-24689	An issue was discovered in DSK DSKNet 2.16.136.0 and 2.17.136.5. It mishandles access control. This allows a remote attacker to access account information pages (including personal data) without being authenticated. The collected information includes the badge numbers that operate as user login names. They have a PIN code. The PIN code is 4 digits and thus can be guessed in 10000 brute force attempts.
CVE-2022-25858	The package terser before 4.8.1, from 5.0.0 and before 5.14.2 are vulnerable to Regular Expression Denial of Service (ReDoS) due to insecure usage of regular expressions.

CVE Number	Description
CVE-2022-21549	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 17.0.3.1; Oracle GraalVM Enterprise Edition: 21.3.2 and 22.1.0. Easily exploitable 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 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).
CVE-2022-30622	Disclosure of information - the system allows you to view usernames and passwords without permissions, thus it will be possible to enter the system. Path access: http://api/sys_username_passwd.cmd - The server loads the request clearly by default. Disclosure of hard-coded credit information within the JS code sent to the customer within the Login.js file is a strong user (which is not documented) and also the password, which allow for super-user access. Username: chcadmin, Password: chcpassword.
CVE-2022-34758	A CWE-20: Improper Input Validation vulnerability exists that could cause the device watchdog function to be disabled if the attacker had access to privileged user credentials. Affected Products: Easergy P5 (V01.401.102 and prior)
CVE-2022-21539	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.29 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 5.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2022-27544	BigFix Web Reports authorized users may see SMTP credentials in clear text.
CVE-2022-21537	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 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).
CVE-2022-21547	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). 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).
CVE-2022-21534	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). 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).
CVE-2022-21553	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).
CVE-2022-21526	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).
CVE-2022-21531	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).
CVE-2022-21530	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).
CVE-2022-21529	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).
CVE-2022-21455	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PAM Auth Plugin). 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 creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).
CVE-2022-21525	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).

CVE Number	Description
CVE-2022-21521	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: XML Publisher). Supported versions that are affected are 8.58 and 8.59. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP 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 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).
CVE-2022-21517	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 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).
CVE-2022-21515	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.38 and prior and 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).
CVE-2022-2222	The Download Monitor WordPress plugin before 4.5.91 does not ensure that files to be downloaded are inside the blog folders, and not sensitive, allowing high privilege users such as admin to download the wp-config.php or /etc/passwd even in an hardened environment or multisite setup.
CVE-2022-2186	The Simple Post Notes WordPress plugin before 1.7.6 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
CVE-2022-2099	The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles
CVE-2020-21967	File upload vulnerability in the Catalog feature in Prestashop 1.7.6.7 allows remote attackers to run arbitrary code via the add new file page.
CVE-2022-2100	The Page Generator WordPress plugin before 1.6.5 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
CVE-2022-2114	The Data Tables Generator by Supsystic WordPress plugin before 1.10.20 does not sanitise and escape some of its Table settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)
CVE-2022-2118	The 404s WordPress plugin before 3.5.1 does not sanitise and escape its fields, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
CVE-2022-2148	The LinkedIn Company Updates WordPress plugin through 1.5.3 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
CVE-2022-2151	The Best Contact Management Software WordPress plugin through 3.7.3 does not sanitise and escape its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
CVE-2022-2169	The Loading Page with Loading Screen WordPress plugin before 1.0.83 does not escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
CVE-2022-2149	The Very Simple Breadcrumb WordPress plugin through 1.0 does not sanitise and escape its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
CVE-2022-2194	The Accept Stripe Payments WordPress plugin before 2.0.64 does not sanitize and escape some of its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
CVE-2022-23438	An improper neutralization of input during web page generation ('Cross-site Scripting') [CWE-79] vulnerability in FortiOS version 7.0.5 and prior and 6.4.9 and prior may allow an unauthenticated remote attacker to perform a reflected cross site scripting (XSS) attack in the captive portal authentication replacement page.
CVE-2022-27545	BigFix Web Reports authorized users may perform HTML injection for the email administrative configuration page.
CVE-2022-1984	This issue affects: HYPR Windows WFA versions prior to 7.2; Unsafe Deserialization vulnerability in HYPR Workforce Access (WFA) before version 7.2 may allow local authenticated attackers to elevate privileges via a malicious serialized payload.

CVE Number	Description
CVE-2022-21522	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.29 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).
CVE-2022-21512	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Integration Broker). Supported versions that are affected are 8.58 and 8.59. Easily exploitable vulnerability allows high 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 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2021-26382	An attacker with root account privileges can load any legitimately signed firmware image into the Audio Co-Processor (ACP,) irrespective of the respective signing key being declared as usable for authenticating an ACP firmware image, potentially resulting in a denial of service.
CVE-2022-21554	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.36. 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).
CVE-2022-21523	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: BI Publisher Security). 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 BI Publisher. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle BI Publisher 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).
CVE-2022-21532	Vulnerability in the JD Edwards EnterpriseOne Orchestrator product of Oracle JD Edwards (component: E1 IOT Orchestrator). Supported versions that are affected are 9.2.6.3 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Orchestrator 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).
CVE-2022-2144	The Jquery Validation For Contact Form 7 WordPress plugin before 5.3 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change Blog options like default_role, users_can_register via a CSRF attack
CVE-2022-28876	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant and in certain WithSecure products whereby the scanning the aeheur.dll component can crash the scanning engine. The exploit can be triggered remotely by an attacker.
CVE-2021-39018	IBM Engineering Lifecycle Optimization - Publishing 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 could disclose sensitive information in a SQL error message that could aid in further attacks against the system. IBM X-Force ID: 213726.
CVE-2022-2408	The Guest account feature in Mattermost version 6.7.0 and earlier fails to properly restrict the permissions, which allows a guest user to fetch a list of all public channels in the team, in spite of not being part of those channels.
CVE-2021-42755	An integer overflow / wraparound vulnerability [CWE-190] in FortiSwitch 7.0.2 and below, 6.4.9 and below, 6.2.x, 6.0.x; FortiRecorder 6.4.2 and below, 6.0.10 and below; FortiOS 7.0.2 and below, 6.4.8 and below, 6.2.10 and below, 6.0.x; FortiProxy 7.0.0, 2.0.6 and below, 1.2.x, 1.1.x, 1.0.x; FortiVoiceEnterprise 6.4.3 and below, 6.0.10 and below dhcpd daemon may allow an unauthenticated and network adjacent attacker to crash the dhcpd deamon, resulting in potential denial of service.
CVE-2022-2406	The legacy Slack import feature in Mattermost version 6.7.0 and earlier fails to properly limit the sizes of imported files, which allows an authenticated attacker to crash the server by importing large files via the Slack import REST API.
CVE-2021-39016	IBM Engineering Lifecycle Optimization - Publishing 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2 does not sufficiently monitor or control transmitted network traffic volume, so that an actor can cause the software to transmit more traffic than should be allowed for that actor. IBM X-Force ID: 213722.
CVE-2015-10003	A vulnerability, which was classified as problematic, was found in FileZilla Server up to 0.9.50. This affects an unknown part of the component PORT Handler. The manipulation leads to unintended intermediary. It is possible to initiate the attack remotely. Upgrading to version 0.9.51 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2022-25869	All versions of package angular are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.
CVE-2022-21439	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows high 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 ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H).
CVE-2022-21555	Vulnerability in the MySQL Shell for VS Code product of Oracle MySQL (component: Shell: GUI). Supported versions that are affected are 1.1.8 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Shell for VS Code executes to compromise MySQL Shell for VS Code. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Shell for VS Code, 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 MySQL Shell for VS Code accessible data as well as unauthorized read access to a subset of MySQL Shell for VS Code accessible data. CVSS 3.1 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).

CVE Number	Description
CVE-2022-2394	Puppet Bolt prior to version 3.24.0 will print sensitive parameters when planning a run resulting in them potentially being logged when run programmatically, such as via Puppet Enterprise.
CVE-2020-7641	This affects all versions of package grunt-util-property. The function call could be tricked into adding or modifying properties of Object.prototype using a __proto__ payload.
CVE-2022-20226	In finishDrawingWindow of WindowManagerService.java, there is a possible tapjacking due to improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-213644870
CVE-2022-2469	GNU SASL libgsasl server-side read-out-of-bounds with malicious authenticated GSS-API client
CVE-2022-22450	IBM Security Verify Identity Manager 10.0 could allow a privileged user to upload a malicious file by bypassing extension security in an HTTP request. IBM X-Force ID: 224916.
CVE-2022-2396	A vulnerability classified as problematic was found in SourceCodester Simple e-Learning System 1.0. Affected by this vulnerability is an unknown functionality of the file /vcs/claire_blake. The manipulation of the argument Bio with the input "><script>alert(document.cookie)</script> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-21563	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 3.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L).
CVE-2022-34874	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.2.53575. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. By performing actions in JavaScript, an attacker can trigger a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-17474.
CVE-2022-34875	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of ADBC objects. By performing actions in JavaScript, an attacker can trigger a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-16981.
CVE-2022-35906	An issue was discovered in Bentley MicroStation before 10.17.0.x and Bentley View before 10.17.0.x. Using an affected version of MicroStation or MicroStation-based application to open a DGN file containing crafted data can force an out-of-bounds read. Exploitation of these vulnerabilities within the parsing of DGN files could enable an attacker to read information in the context of the current process.
CVE-2022-35905	An issue was discovered in Bentley MicroStation before 10.17.0.x and Bentley View before 10.17.0.x. Using an affected version of MicroStation or MicroStation-based application to open an FBX file containing crafted data can force an out-of-bounds read. Exploitation of these vulnerabilities within the parsing of FBX files could enable an attacker to read information in the context of the current process.
CVE-2022-35904	An issue was discovered in Bentley MicroStation before 10.17.0.x and Bentley View before 10.17.0.x. Using an affected version of MicroStation or MicroStation-based application to open an IFC file containing crafted data can force an out-of-bounds read. Exploitation of these vulnerabilities within the parsing of IFC files could enable an attacker to read information in the context of the current process.
CVE-2022-35903	An issue was discovered in Bentley MicroStation before 10.17.0.x and Bentley View before 10.17.0.x. Using an affected version of MicroStation or MicroStation-based application to open a 3DS file containing crafted data can force an out-of-bounds read. Exploitation of these vulnerabilities within the parsing of 3DS files could enable an attacker to read information in the context of the current process.
CVE-2022-35902	An issue was discovered in Bentley MicroStation before 10.17.0.x and Bentley View before 10.17.0.x. Using an affected version of MicroStation or MicroStation-based application to open an OBJ file containing crafted data can force an out-of-bounds read. Exploitation of these vulnerabilities within the parsing of OBJ files could enable an attacker to read information in the context of the current process.
CVE-2022-35901	An issue was discovered in Bentley MicroStation before 10.17.0.x and Bentley View before 10.17.0.x. Using an affected version of MicroStation or MicroStation-based application to open a J2K file containing crafted data can force an out-of-bounds read. Exploitation of these vulnerabilities within the parsing of J2K files could enable an attacker to read information in the context of the current process.
CVE-2022-35900	An issue was discovered in Bentley MicroStation before 10.17.0.x and Bentley View before 10.17.0.x. Using an affected version of MicroStation or MicroStation-based application to open a JP2 file containing crafted data can force an out-of-bounds read. Exploitation of these vulnerabilities within the parsing of JP2 files could enable an attacker to read information in the context of the current process.
CVE-2022-34873	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. By performing actions in JavaScript, an attacker can trigger a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-16777.

CVE Number	Description
CVE-2022-21538	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.29 and prior. Difficult to exploit 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-21432	Vulnerability in the Oracle Database - Enterprise Edition RDBMS Security component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 19c and 21c. Easily exploitable vulnerability allows high privileged attacker having DBA role privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition RDBMS Security. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Database - Enterprise Edition RDBMS Security. 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).
CVE-2022-21535	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell: General/Core Client). Supported versions that are affected are 8.0.28 and prior. Difficult to exploit vulnerability allows unauthenticated 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 ability to cause a partial denial of service (partial DOS) of MySQL Shell. CVSS 3.1 Base Score 2.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).
CVE-2020-35259	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
CVE-2021-27294	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
CVE-2020-35257	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