الهيئة الوطنية
للأمن السيبراني
Nat onal Cybersecurity Authority

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 15th of April to 22nd of April. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- **Critical: CVSS base score of 9.0-10.0**
- **High: CVSS base score of 7.0-8.9**
- **Medium: CVSS base score 4.0-6.9**
- **Low: CVSS base score 0.0-3.9**

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ١٥ أبريل إلى ٢٢ أبريل. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدّا: النتيجة الأساسية لـCVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـCVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـCVSS 4.0-6.9**
- **منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-22946	apache - spark	In Apache Spark versions prior to 3.4.0, applications using spark-submit can specify a 'proxy-user' to run as, limiting privileges. The application can execute code with the privileges of the submitting user, however, by providing malicious configuration-related classes on the classpath. This affects architectures relying on proxy-user, for example those using Apache Livy to manage submitted applications. Update to Apache Spark 3.4.0 or later, and ensure that spark.submit.proxyUser.allowCustomClasspathInClusterMode is set to its default of "false", and is not overridden by submitted applications.	2023-04-17	9.9	Critical
CVE-2021-46880	openbsd - multiple products	x509/x509_verify.c in LibreSSL before 3.4.2, and OpenBSD before 7.0 errata 006, allows authentication bypass because an error for an unverified certificate chain is sometimes discarded.	2023-04-15	9.8	Critical
CVE-2021-33990	liferay - liferay_portal	** DISPUTED ** Liferay Portal 6.2.5 allows Command=FileUpload&Type=File&CurrentFolder=/ requests when frmfolders.html exists. NOTE: The vendor disputes this issue because the exploit reference link only shows frmfolders.html is accessible and does not demonstrate how an unauthorized user can upload a file.	2023-04-16	9.8	Critical
CVE-2023-24831	apache - iotdb	Improper Authentication vulnerability in Apache Software Foundation Apache IoTDB.This issue affects Apache IoTDB Grafana Connector: from 0.13.0 through 0.13.3. Attackers could login without authorization. This is fixed in 0.13.4.	2023-04-17	9.8	Critical
CVE-2023-30771	apache - iotdb	Incorrect Authorization vulnerability in Apache Software Foundation Apache IoTDB.This issue affects the iotdb-web-workbench component on 0.13.3. iotdb-web-workbench is an optional component of IoTDB, providing a web console of the database. This problem is fixed from version 0.13.4 of iotdb-web-workbench onwards.	2023-04-17	9.8	Critical
CVE-2023-28962	juniper - multiple products	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.	2023-04-17	9.8	Critical

CVE-2023-25549	schneider-electric - struxureware_data_center_expert	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that allows for remote code execution when using a parameter of the DCE network settings endpoint. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	2023-04-18	9.8	Critical
CVE-2023-25550	schneider-electric - struxureware_data_center_expert	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that allows remote code execution via the “hostname” parameter when maliciously crafted hostname syntax is entered. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	2023-04-18	9.8	Critical
CVE-2023-29411	schneider-electric - apc_easy_ups_online_monitoring_software	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow changes to administrative credentials, leading to potential remote code execution without requiring prior authentication on the Java RMI interface.	2023-04-18	9.8	Critical
CVE-2023-29412	schneider-electric - apc_easy_ups_online_monitoring_software	A CWE-78: Improper Handling of Case Sensitivity vulnerability exists that could cause remote code execution when manipulating internal methods through Java RMI interface.	2023-04-18	9.8	Critical
CVE-2023-28004	schneider-electric - powerlogic_hdpm6000_firmware	A CWE-129: Improper validation of an array index vulnerability exists where a specially crafted Ethernet request could result in denial of service or remote code execution.	2023-04-18	9.8	Critical

CVE-2023-21096	google - multiple products	In OnWakelockReleased of attribution_processor.cc, there is a use after free that could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-254774758	2023-04-19	9.8	Critical
CVE-2023-2136	google - chrome	Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2023-04-19	9.6	Critical
CVE-2022-48312	huawei - multiple products	The HwPCAssistant module has the out-of-bounds read/write vulnerability. Successful exploitation of this vulnerability may affect confidentiality and integrity.	2023-04-16	9.1	Critical
CVE-2023-27976	schneider-electric - ecostruxure_control_expert	A CWE-668: Exposure of Resource to Wrong Sphere vulnerability exists that could cause remote code execution when a valid user visits a malicious link provided through the web endpoints. Affected Products: EcoStruxure Control Expert (V15.1 and above)	2023-04-18	8.8	High
CVE-2023-25556	schneider-electric - merten_instabus_tastermodul_1fach_system_m_firmware	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation.	2023-04-18	8.8	High
CVE-2023-25547	schneider-electric - struxureware_data_center_expert	A CWE-863: Incorrect Authorization vulnerability exists that could allow remote code execution on upload and install packages when a hacker is using a low privileged user account. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	2023-04-18	8.8	High
CVE-2023-29410	schneider-electric - multiple products	A CWE-20: Improper Input Validation vulnerability exists that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is provided over HTTP for the server to execute.	2023-04-18	8.8	High
CVE-2023-2133	google - chrome	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-04-19	8.8	High
CVE-2023-2134	google - chrome	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-04-19	8.8	High
CVE-2023-2137	google - chrome	Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-04-19	8.8	High
CVE-2023-21085	google - multiple products	In nci_snd_set_routing_cmd of nci_hmsgs.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-264879662	2023-04-19	8.8	High
CVE-2023-21923	oracle - multiple products	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Health Sciences InForm accessible data as well as unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L).	2023-04-18	8.3	High
CVE-2023-28960	juniper - multiple products	An Incorrect Permission Assignment for Critical Resource vulnerability in Juniper Networks Junos OS Evolved allows a local, authenticated low-privileged attacker to copy potentially malicious files into an existing Docker container on the local system. A follow-on administrator could then inadvertently start the Docker container leading to the malicious files being executed as root.	2023-04-17	8.2	High

		This issue only affects systems with Docker configured and enabled, which is not enabled by default. Systems without Docker started are not vulnerable to this issue. This issue affects Juniper Networks Junos OS Evolved: 20.4 versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO.			
CVE-2023-21990	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. 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).	2023-04-18	8.2	High
CVE-2023-25552	schneider-electric - struxureware_data_center_expert	A CWE-862: Missing Authorization vulnerability exists that could allow viewing of unauthorized content, changes or deleting of content, or performing unauthorized functions when tampering the Device File Transfer settings on DCE endpoints. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	2023-04-18	8.1	High
CVE-2023-25555	schneider-electric - struxureware_data_center_expert	A CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could allow a user that knows the credentials to execute unprivileged shell commands on the appliance over SSH. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	2023-04-18	8.1	High
CVE-2023-28966	juniper - multiple products	An Incorrect Default Permissions vulnerability in Juniper Networks Junos OS Evolved allows a low-privileged local attacker with shell access to modify existing files or execute commands as root. The issue is caused by improper file and directory permissions on certain system files, allowing an attacker with access to these files and folders to inject CLI commands as root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO.	2023-04-17	7.8	High
CVE-2023-21948	oracle - solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Core). The supported version that is affected is 10.	2023-04-18	7.8	High

		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 takeover of Oracle Solaris. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
CVE-2023-21987	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. 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).	2023-04-18	7.8	High
CVE-2023-25554	schneider-electric - struxureware_data_center_expert	A CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that allows a local privilege escalation on the appliance when a maliciously crafted Operating System command is entered on the device. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	2023-04-18	7.8	High
CVE-2021-0872	google - android	In PVRSRVBridgeRGXKickVRDM of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270401229	2023-04-19	7.8	High
CVE-2021-0873	google - android	In PVRSRVBridgeRGXKickRS of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270392711	2023-04-19	7.8	High
CVE-2021-0874	google - android	In PVRSRVBridgeDevicememHistorySparseChange of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270399633	2023-04-19	7.8	High
CVE-2021-0875	google - android	In PVRSRVBridgeChangeSparseMem of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270400061	2023-04-19	7.8	High
CVE-2021-0876	google - android	In PVRSRVBridgePhysmemNewRamBackedLockedPMR of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270400229	2023-04-19	7.8	High
CVE-2021-0878	google - android	In PVRSRVBridgeServerSyncGetStatus of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270399153	2023-04-19	7.8	High
CVE-2021-0879	google - android	In PVRSRVBridgeRGXTDMSubmitTransfer of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	2023-04-19	7.8	High

		exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270397970			
CVE-2021-0880	google - android	In PVRSRVBridgeRGXKickTA3D of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270396792	2023-04-19	7.8	High
CVE-2021-0881	google - android	In PVRSRVBridgeRGXKickCDM of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270396350	2023-04-19	7.8	High
CVE-2021-0882	google - android	In PVRSRVBridgeRGXKickSync of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270395803	2023-04-19	7.8	High
CVE-2021-0883	google - android	In PVRSRVBridgeCacheOpQueue of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270395013	2023-04-19	7.8	High
CVE-2021-0884	google - android	In PVRSRVBridgePhysmemImportSparseDmaBuf of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270393454	2023-04-19	7.8	High
CVE-2021-0885	google - android	In PVRSRVBridgeSyncPrimOpTake of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-270401914	2023-04-19	7.8	High
CVE-2023-20950	google - multiple products	In AlarmManagerActivity of AlarmManagerActivity.java, there is a possible way to bypass background activity launch restrictions via a pendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-195756028	2023-04-19	7.8	High
CVE-2023-20967	google - multiple products	In avdt_scb_hdl_pkt_no_frag of avdt_scb_act.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-225879503	2023-04-19	7.8	High
CVE-2023-21081	google - multiple products	In multiple functions of PackageInstallerService.java and related files, there is a possible way to bypass background activity launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-230492955	2023-04-19	7.8	High
CVE-2023-21083	google - multiple products	In onNullBinding of CallScreeningServiceHelper.java, there is a possible way to record audio without showing a privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-252762941	2023-04-19	7.8	High
CVE-2023-21086	google - multiple products	In isToggleable of SecureNfcEnabler.java and SecureNfcPreferenceController.java, there is a possible way to enable NFC from a secondary account due to a permissions bypass. This could lead to local escalation of privilege from the Guest account with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-238298970	2023-04-19	7.8	High
CVE-2023-21088	google - multiple products	In deliverOnFlushComplete of LocationProviderManager.java, there is a possible way to bypass background activity launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-235823542	2023-04-19	7.8	High

CVE-2023-21089	google - multiple products	In startInstrumentation of ActivityManagerService.java, there is a possible way to keep the foreground service alive while the app is in the background. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-237766679	2023-04-19	7.8	High
CVE-2023-21092	google - multiple products	In retrieveServiceLocked of ActiveServices.java, there is a possible way to dynamically register a BroadcastReceiver using permissions of System App due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242040055	2023-04-19	7.8	High
CVE-2023-21093	google - multiple products	In extractRelativePath of FileUtils.java, there is a possible way to access files in a directory belonging to other applications due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-228450832	2023-04-19	7.8	High
CVE-2023-21094	google - multiple products	In sanitize of LayerState.cpp, there is a possible way to take over the screen display and swap the display content due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-248031255	2023-04-19	7.8	High
CVE-2023-21097	google - multiple products	In toUriInner of Intent.java, there is a possible way to launch an arbitrary activity 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-11 Android-12 Android-12L Android-13Android ID: A-261858325	2023-04-19	7.8	High
CVE-2023-21098	google - multiple products	In multiple functions of AccountManagerService.java, there is a possible loading of arbitrary code into the System Settings app 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-11 Android-12 Android-12L Android-13Android ID: A-260567867	2023-04-19	7.8	High
CVE-2023-21099	google - multiple products	In multiple methods of PackageInstallerSession.java, there is a possible way to start foreground services from the background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-243377226	2023-04-19	7.8	High
CVE-2023-21100	google - multiple products	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-242544249	2023-04-19	7.8	High
CVE-2023-28047	dell - display_manager	Dell Display Manager, versions 2.1.0 and prior, contains an arbitrary file or folder creation vulnerability during installation. A local low privilege attacker could potentially exploit this vulnerability, leading to the execution of arbitrary code on the operating system with high privileges.	2023-04-20	7.8	High
CVE-2023-21985	oracle - multiple products	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). 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 and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H).	2023-04-18	7.7	High
CVE-2022-37255	tp-link - tapo_c310_firmware	TP-Link Tapo C310 1.3.0 devices allow access to the RTSP video feed via credentials of User --- and Password TPL075526460603.	2023-04-16	7.5	High
CVE-2023-28964	juniper - multiple products	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks	2023-04-17	7.5	High

		Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO;			
CVE-2023-28965	juniper - multiple products	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2.	2023-04-17	7.5	High
CVE-2023-28967	juniper - multiple products	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO.	2023-04-17	7.5	High
CVE-2022-43377	schneider-electric - netbotz_355_firmware	A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could cause account takeover when a brute force attack is performed on the account. Affected Products: NetBotz 4 - 355/450/455/550/570 (V4.7.0 and prior)	2023-04-18	7.5	High
CVE-2023-21912	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.41 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows unauthenticated 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 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).	2023-04-18	7.5	High
CVE-2023-21931	oracle - multiple products	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 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server 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).	2023-04-18	7.5	High
CVE-2023-21964	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that	2023-04-18	7.5	High

		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 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. 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-2023-21979	oracle - multiple products	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 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server 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).	2023-04-18	7.5	High
CVE-2023-21996	oracle - multiple products	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 HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. 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).	2023-04-18	7.5	High
CVE-2023-29413	schneider-electric - apc_easy_ups_online_monitoring_software	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause Denial-of-Service when accessed by an unauthenticated user on the Schneider UPS Monitor service.	2023-04-18	7.5	High
CVE-2023-2135	google - chrome	Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to enable specific preconditions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-04-19	7.5	High
CVE-2023-25619	schneider-electric - modicon_m580_firmware	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol.	2023-04-19	7.5	High
CVE-2023-21930	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS 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 as well as unauthorized access to critical data or complete access to 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 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2023-04-18	7.4	High
CVE-2023-28971	juniper - paragon_active_assurance	An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in the timescaledb feature of Juniper Networks Paragon Active Assurance (PAA) (Formerly Netrounds) allows an attacker to bypass existing firewall rules and limitations used to restrict internal communcations. The Test Agents (TA) Appliance connects to the Control Center (CC) using OpenVPN. TA's are assigned an internal IP address in the 100.70.0.0/16 range. Firewall rules exists to limit communication from TA's to the CC to specific services only. OpenVPN is configured to not allow direct communication between Test Agents in the OpenVPN	2023-04-17	7.2	High

		application itself, and routing is normally not enabled on the server running the CC application. The timescaledb feature is installed as an optional package on the Control Center. When the timescaledb container is started, this causes side-effects by bypassing the existing firewall rules and limitations for Test Agent communications. Note: This issue only affects customers hosting their own on-prem Control Center. The Paragon Active Assurance Software as a Service (SaaS) is not affected by this vulnerability since the timescaledb service is not enabled. This issue affects all on-prem versions of Juniper Networks Paragon Active Assurance prior to 4.1.2.			
CVE-2023-21932	oracle - hospitality_opera_5_property_services	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: OXI). The supported version that is affected is 5.6. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. While the vulnerability is in Oracle Hospitality OPERA 5 Property Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality OPERA 5 Property Services accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L).	2023-04-18	7.2	High
CVE-2023-28973	juniper - multiple products	An Improper Authorization vulnerability in the 'sysmanctl' shell command of Juniper Networks Junos OS Evolved allows a local, authenticated attacker to execute administrative commands that could impact the integrity of the system or system availability. Administrative functions such as daemon restarting, routing engine (RE) switchover, and node shutdown can all be performed through exploitation of the 'sysmanctl' command. Access to the 'sysmanctl' command is only available from the Junos shell. Neither direct nor indirect access to 'sysmanctl' is available from the Junos CLI. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO; 21.4 versions prior to 21.4R1-S2-EVO, 21.4R2-EVO.	2023-04-17	7.1	High
CVE-2023-21980	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. 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).	2023-04-18	7.1	High
CVE-2023-21896	oracle - multiple products	Vulnerability in the Oracle Solaris product of Oracle Systems (component: NSSwitch). Supported versions that are affected are 10 and 11. Difficult to exploit 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 takeover of Oracle Solaris. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2023-04-18	7	High
CVE-2023-28972	juniper - multiple products	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.	2023-04-17	6.8	Medium

CVE-2023-21918	oracle - multiple products	Vulnerability in the Oracle Database Recovery Manager component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows high privileged attacker having Local SYSDBA privilege with network access via Oracle Net to compromise Oracle Database Recovery Manager. While the vulnerability is in Oracle Database Recovery Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Database Recovery Manager. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	2023-04-18	6.8	Medium
CVE-2023-21922	oracle - multiple products	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Health Sciences InForm. 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 Health Sciences InForm accessible data as well as unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N).	2023-04-18	6.8	Medium
CVE-2023-21934	oracle - multiple products	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Difficult to exploit vulnerability allows low privileged attacker having User Account privilege with network access via TLS 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 as well as unauthorized access to critical data or complete access to all Java VM accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N).	2023-04-18	6.8	Medium
CVE-2022-34755	schneider-electric - easergy_builder_installer	A CWE-427 - Uncontrolled Search Path Element vulnerability exists that could allow an attacker with a local privileged account to place a specially crafted file on the target machine, which may give the attacker the ability to execute arbitrary code during the installation process initiated by a valid user. Affected Products: Easergy Builder Installer (1.7.23 and prior)	2023-04-18	6.7	Medium
CVE-2023-21969	oracle - sql_developer	Vulnerability in Oracle SQL Developer (component: Installation). Supported versions that are affected are Prior to 23.1.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle SQL Developer executes to compromise Oracle SQL Developer. Successful attacks of this vulnerability can result in takeover of Oracle SQL Developer. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2023-04-18	6.7	Medium
CVE-2023-21084	google - android	In buildPropFile of filesystem.go, there is a possible insecure hash due to an improperly used crypto. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262892300	2023-04-19	6.7	Medium
CVE-2023-2194	linux - multiple products	An out-of-bounds write vulnerability was found in the Linux kernel's SLIMpro I2C device driver. The userspace "data->block[0]" variable was not capped to a number between 0-255 and was used as the size of a memcpy, possibly writing beyond the end of dma_buffer. This flaw could allow a local privileged user to crash the system or potentially achieve code execution.	2023-04-20	6.7	Medium
CVE-2023-20941	google - android	In acc_ctrlrequest_composite of f_accessory.c, there is a possible out of bounds write due to a missing bounds check. This could lead to physical escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-264029575References: Upstream kernel	2023-04-19	6.6	Medium
CVE-2022-48313	huawei - multiple products	The Bluetooth module has a vulnerability of bypassing the user confirmation in the pairing process. Successful exploitation of this vulnerability may affect confidentiality.	2023-04-16	6.5	Medium
CVE-2022-48314	huawei - multiple products	The Bluetooth module has a vulnerability of bypassing the user confirmation in the pairing process. Successful exploitation of this vulnerability may affect confidentiality.	2023-04-16	6.5	Medium

CVE-2023-25504	apache - superset	A malicious actor who has been authenticated and granted specific permissions in Apache Superset may use the import dataset feature in order to conduct Server-Side Request Forgery attacks and query internal resources on behalf of the server where Superset is deployed. This vulnerability exists in Apache Superset versions up to and including 2.0.1.	2023-04-17	6.5	Medium
CVE-2023-1697	juniper - multiple products	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2.	2023-04-17	6.5	Medium
CVE-2023-28959	juniper - multiple products	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.	2023-04-17	6.5	Medium
CVE-2023-28970	juniper - multiple products	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing on the network interfaces of Juniper Networks Junos OS on JRR200 route reflector appliances allows an adjacent, network-based attacker sending a specific packet to the device to cause a kernel crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by an attacker on the local broadcast domain. Packets routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2.	2023-04-17	6.5	Medium

CVE-2023-28974	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2.	2023-04-17	6.5	Medium
CVE-2023-21909	oracle - siebel_crm	Vulnerability in the Siebel CRM product of Oracle Siebel CRM (component: UI Framework). Supported versions that are affected are 23.3 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM 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).	2023-04-18	6.5	Medium
CVE-2023-21910	oracle - multiple products	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web General). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 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).	2023-04-18	6.5	Medium
CVE-2023-21946	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 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).	2023-04-18	6.5	Medium
CVE-2023-21978	oracle - application_object_library	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: GUI). 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 Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, 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 Application Object Library accessible data as well as unauthorized read access to a subset of Oracle Application Object Library accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Object Library. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L).	2023-04-18	6.5	Medium
CVE-2023-21984	oracle - solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Libraries). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP 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 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).	2023-04-18	6.5	Medium
CVE-2023-21993	oracle - clinical_remote_data_capture	Vulnerability in the Oracle Clinical Remote Data Capture product of Oracle Health Sciences Applications (component: Forms). The supported version that is affected is 5.4.0.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Clinical Remote Data Capture. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Clinical	2023-04-18	6.5	Medium

		Remote Data Capture 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-2022-43378	schneider-electric - netbotz_355_firmware	A CWE-1021: Improper Restriction of Rendered UI Layers or Frames vulnerability exists that could cause the user to be tricked into performing unintended actions when external address frames are not properly restricted. Affected Products: NetBotz 4 - 355/450/455/550/570 (V4.7.0 and prior)	2023-04-18	6.5	Medium
CVE-2023-25548	schneider-electric - struxureware_data_center_expert	A CWE-863: Incorrect Authorization vulnerability exists that could allow access to device credentials on specific DCE endpoints not being properly secured when a hacker is using a low privileged user. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	2023-04-18	6.5	Medium
CVE-2023-25620	schneider-electric - modicon_m580_firmware	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user.	2023-04-19	6.5	Medium
CVE-2023-30772	linux - linux_kernel	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/power/supply/da9150-charger.c if a physically proximate attacker unplugs a device.	2023-04-16	6.4	Medium
CVE-2021-34337	gnu - mailman	An issue was discovered in Mailman Core before 3.3.5. An attacker with access to the REST API could use timing attacks to determine the value of the configured REST API password and then make arbitrary REST API calls. The REST API is bound to localhost by default, limiting the ability for attackers to exploit this, but can optionally be made to listen on other interfaces.	2023-04-15	6.3	Medium
CVE-2022-43376	schneider-electric - netbotz_355_firmware	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause code and session manipulation when malicious code is inserted into the browser. Affected Products: NetBotz 4 - 355/450/455/550/570 (V4.7.0 and prior)	2023-04-18	6.1	Medium
CVE-2023-21905	oracle - multiple products	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: Routing Hub). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. 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 Virtual Account Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N).	2023-04-18	6.1	Medium
CVE-2023-21906	oracle - multiple products	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: SMS Module). Supported versions that are affected are 14.5, 14.6 and	2023-04-18	6.1	Medium

		14.7. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. 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 Virtual Account Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N).			
CVE-2023-21956	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server 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).	2023-04-18	6.1	Medium
CVE-2023-25551	schneider-electric - struxureware_data_center_expert	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists on a DCE file upload endpoint when tampering with parameters over HTTP. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)	2023-04-18	6.1	Medium
CVE-2023-25553	schneider-electric - struxureware_data_center_expert	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists on a DCE endpoint through the logging capabilities of the webserver.	2023-04-18	6.1	Medium

		Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)			
CVE-2023-21907	oracle - multiple products	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. 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 Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:H).	2023-04-18	6	Medium
CVE-2023-21908	oracle - multiple products	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. 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 Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:H).	2023-04-18	6	Medium
CVE-2023-21989	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2023-04-18	6	Medium
CVE-2023-22002	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2023-04-18	6	Medium
CVE-2023-21924	oracle - multiple products	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Health Sciences InForm, 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 Health Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Health Sciences InForm accessible data and unauthorized	2023-04-18	5.9	Medium

		ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L).			
CVE-2023-21954	oracle - multiple products	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: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. 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 access to critical data or complete access to 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 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2023-04-18	5.9	Medium
CVE-2023-21967	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	2023-04-18	5.9	Medium
CVE-2023-21952	oracle - business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N).	2023-04-18	5.7	Medium
CVE-2023-21965	oracle - business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N).	2023-04-18	5.7	Medium
CVE-2023-21970	oracle - bi_publisher	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Security). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. 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 BI Publisher accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N).	2023-04-18	5.7	Medium
CVE-2023-21986	oracle - multiple products	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Native Image). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where	2023-04-18	5.7	Medium

		Oracle GraalVM Enterprise Edition executes to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, 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 GraalVM Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.1 Base Score 5.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L).			
CVE-2023-21960	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP 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 as well as unauthorized read access to a subset 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 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).	2023-04-18	5.6	Medium
CVE-2023-1548	schneider-electric - ecostruxure_control_expert	A CWE-269: Improper Privilege Management vulnerability exists that could cause a local user to perform a denial of service through the console server service that is part of EcoStruxure Control Expert. Affected Products: EcoStruxure Control Expert (V15.1 and above)	2023-04-18	5.5	Medium
CVE-2023-21926	oracle - multiple products	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Health Sciences InForm executes to compromise Oracle Health Sciences InForm. 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 Health Sciences InForm accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N).	2023-04-18	5.5	Medium
CVE-2023-21929	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.32 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).	2023-04-18	5.5	Medium
CVE-2023-20909	google - multiple products	In multiple functions of RunningTasks.java, there is a possible privilege escalation due to a missing privilege check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-243130512	2023-04-19	5.5	Medium
CVE-2023-20935	google - multiple products	In deserialize of multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-256589724	2023-04-19	5.5	Medium
CVE-2023-21080	google - multiple products	In register_notification_rsp of btif_rc.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245916076	2023-04-19	5.5	Medium
CVE-2023-21082	google - multiple products	In getNumberFromCallIntent of NewOutgoingCallIntentBroadcaster.java, there is a possible way to enumerate other user's contact phone number due to a confused deputy. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-257030107	2023-04-19	5.5	Medium
CVE-2023-21087	google - multiple products	In PreferencesHelper.java, an uncaught exception may cause the device to get stuck in a boot loop. This could lead to local persistent denial of service with no additional execution privileges	2023-04-19	5.5	Medium

		needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261723753			
CVE-2023-21091	google - android	In canDisplayLocalUi of AppLocalePickerActivity.java, there is a possible way to change system app locales due to a missing permission check. This could lead to local denial of service across user boundaries with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257954050	2023-04-19	5.5	Medium
CVE-2023-2162	linux - multiple products	A use-after-free vulnerability was found in iscsi_sw_tcp_session_create in drivers/scsi/iscsi_tcp.c in SCSI sub-component in the Linux Kernel. In this flaw an attacker could leak kernel internal information.	2023-04-19	5.5	Medium
CVE-2023-28327	linux - linux_kernel	A NULL pointer dereference flaw was found in the UNIX protocol in net/unix/diag.c In unix_diag_get_exact in the Linux Kernel. The newly allocated skb does not have sk, leading to a NULL pointer. This flaw allows a local user to crash or potentially cause a denial of service.	2023-04-19	5.5	Medium
CVE-2023-28328	linux - linux_kernel	A NULL pointer dereference flaw was found in the az6027 driver in drivers/media/usb/dev-usb/az6027.c in the Linux Kernel. The message from user space is not checked properly before transferring into the device. This flaw allows a local user to crash the system or potentially cause a denial of service.	2023-04-19	5.5	Medium
CVE-2023-2166	linux - multiple products	A null pointer dereference issue was found in can protocol in net/can/af_can.c in the Linux before Linux. ml_priv may not be initialized in the receive path of CAN frames. A local user could use this flaw to crash the system or potentially cause a denial of service.	2023-04-19	5.5	Medium
CVE-2023-2177	linux - multiple products	A null pointer dereference issue was found in the sctp network protocol in net/sctp/stream_sched.c in Linux Kernel. If stream_in allocation is failed, stream_out is freed which would further be accessed. A local user could use this flaw to crash the system or potentially cause a denial of service.	2023-04-20	5.5	Medium
CVE-2023-21921	oracle - multiple products	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Health Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Health Sciences InForm accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2023-04-18	5.4	Medium
CVE-2023-21936	oracle - jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are Prior to 9.2.7.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2023-04-18	5.4	Medium
CVE-2023-21973	oracle - iprocurement	Vulnerability in the Oracle iProcurement product of Oracle E-Business Suite (component: E-Content Manager Catalog). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iProcurement. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iProcurement, 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 iProcurement accessible data as well as unauthorized read access to a subset of Oracle iProcurement 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).	2023-04-18	5.4	Medium
CVE-2023-21992	oracle - peoplesoft_enterprise_human_capital_management_human_resources	Vulnerability in the PeopleSoft Enterprise HCM Human Resources product of Oracle PeopleSoft (component: Administer Workforce). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human	2023-04-18	5.4	Medium

		Resources. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Human Resources accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).			
CVE-2023-28961	juniper - multiple products	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2.	2023-04-17	5.3	Medium
CVE-2023-28963	juniper - multiple products	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.	2023-04-17	5.3	Medium
CVE-2023-28968	juniper - multiple products	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to	2023-04-17	5.3	Medium

		20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;			
CVE-2023-21903	oracle - multiple products	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Internal Tfr Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. 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 Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:L).	2023-04-18	5.3	Medium
CVE-2023-21904	oracle - multiple products	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. 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 Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:L).	2023-04-18	5.3	Medium
CVE-2023-21916	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Web Server). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2023-04-18	5.3	Medium
CVE-2023-21925	oracle - multiple products	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. 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).	2023-04-18	5.3	Medium
CVE-2023-21939	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized 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).	2023-04-18	5.3	Medium
CVE-2023-21942	oracle - essbase	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result	2023-04-18	5.3	Medium

		in unauthorized access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).			
CVE-2023-21943	oracle - essbase	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP 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 access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).	2023-04-18	5.3	Medium
CVE-2023-21944	oracle - essbase	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP 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 access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).	2023-04-18	5.3	Medium
CVE-2023-21971	oracle - mysql_connectors	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.32 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. 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 MySQL Connectors as well as unauthorized update, insert or delete access to some of MySQL Connectors accessible data and unauthorized read access to a subset of MySQL Connectors accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:H).	2023-04-18	5.3	Medium
CVE-2023-21090	google - android	In parseUsesPermission of ParsingPackageUtils.java, there is a possible boot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-259942609	2023-04-19	5	Medium
CVE-2023-21911	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21913	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 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).	2023-04-18	4.9	Medium
CVE-2023-21917	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2023-04-18	4.9	Medium
CVE-2023-21919	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium

CVE-2023-21920	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21933	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21935	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21945	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21953	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21955	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21962	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21966	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: JSON). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21972	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.32 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	2023-04-18	4.9	Medium

		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-2023-21976	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21977	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-21981	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported versions that are affected are 8.58, 8.59 and 8.60. 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).	2023-04-18	4.9	Medium
CVE-2023-21982	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.9	Medium
CVE-2023-1382	linux - multiple products	A data race flaw was found in the Linux kernel, between where con is allocated and con->sock is set. This issue leads to a NULL pointer dereference when accessing con->sock->sk in net/tipc/topsrv.c in the tipc protocol in the Linux kernel.	2023-04-19	4.7	Medium
CVE-2023-28975	juniper - multiple products	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2.	2023-04-17	4.6	Medium
CVE-2023-21915	oracle - multiple products	Vulnerability in the Oracle Banking Payments product of Oracle Financial Services Applications (component: Book/Internal Transfer). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N).	2023-04-18	4.6	Medium
CVE-2023-21998	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized	2023-04-18	4.6	Medium

		read access to a subset of Oracle VM VirtualBox accessible data. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N).			
CVE-2023-22000	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N).	2023-04-18	4.6	Medium
CVE-2023-22001	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N).	2023-04-18	4.6	Medium
CVE-2023-21940	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.4	Medium
CVE-2023-21947	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 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).	2023-04-18	4.4	Medium
CVE-2023-27525	apache - superset	An authenticated user with Gamma role authorization could have access to metadata information using non trivial methods in Apache Superset up to and including 2.0.1	2023-04-17	4.3	Medium
CVE-2023-21902	oracle - financial_services_behavior_detection_platform	Vulnerability in the Oracle Financial Services Behavior Detection Platform product of Oracle Financial Services Applications (component: Application). The supported version that is affected is 8.0.8.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Behavior Detection Platform. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Financial Services Behavior Detection Platform 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).	2023-04-18	4.3	Medium
CVE-2023-21927	oracle - jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Interoperability SEC). Supported versions that are affected are Prior to 9.2.7.3. 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 read access to a subset of JD Edwards EnterpriseOne Tools 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).	2023-04-18	4.3	Medium
CVE-2023-21941	oracle - multiple products	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0 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).	2023-04-18	4.3	Medium

CVE-2023-21959	oracle - ireceivables	Vulnerability in the Oracle iReceivables product of Oracle E-Business Suite (component: Attachments). Supported versions that are affected are 12.2.3-12.2.12. 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 read access to a subset of Oracle iReceivables 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).	2023-04-18	4.3	Medium
CVE-2023-21997	oracle - user_management	Vulnerability in the Oracle User Management product of Oracle E-Business Suite (component: Proxy User Delegation). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle User Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle User Management 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).	2023-04-18	4.3	Medium
CVE-2023-21988	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2023-04-18	3.8	Low
CVE-2023-21937	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	2023-04-18	3.7	Low
CVE-2023-21938	oracle - multiple products	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: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	2023-04-18	3.7	Low
CVE-2023-21968	oracle - multiple products	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: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or	2023-04-18	3.7	Low

		sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).			
CVE-2023-21999	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Difficult to exploit vulnerability allows low 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 update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N).	2023-04-18	3.6	Low
CVE-2023-22003	oracle - multiple products	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows unauthenticated 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 update, insert or delete access to some of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	2023-04-18	3.3	Low
CVE-2023-21991	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	2023-04-18	3.2	Low
CVE-2023-21963	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 5.7.40 and prior and 8.0.31 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 partial denial of service (partial DOS) of MySQL Server. 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).	2023-04-18	2.7	Low
CVE-2023-21928	oracle - solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: IPS repository daemon). The supported version that is affected is 11. Difficult to exploit 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 update, insert or delete access to some of Oracle Solaris accessible data. CVSS 3.1 Base Score 1.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N).	2023-04-18	1.8	Low

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى
مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.