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

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

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 يوليو إلى ٢٢ يوليو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

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 16th of July to 22nd of July. 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-26512	apache - eventmesh	CWE-502 Deserialization of Untrusted Data at the rabbitmq-connector plugin module in Apache EventMesh (incubating) V1.7.0\V1.8.0 on windows\linux\mac os e.g. platforms allows attackers to send controlled message and remote code execute via rabbitmq messages. Users can use the code under the master branch in project repo to fix this issue, we will release the new version as soon as possible.	2023-07-17	9.8	Critical
CVE-2023-38427	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.8. fs/smb/server/smb2pdu.c in ksmbd has an integer underflow and out-of-bounds read in deassemble_neg_contexts.	2023-07-18	9.8	Critical
CVE-2023-38429	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.4. fs/ksmbd/connection.c in ksmbd has an off-by-one error in memory allocation (because of ksmbd_smb2_check_message) that may lead to out-of-bounds access.	2023-07-18	9.8	Critical
CVE-2023-34034	vmware - multiple products	Using "**" as a pattern in Spring Security configuration for WebFlux creates a mismatch in pattern matching between Spring Security and Spring WebFlux, and the potential for a security bypass.	2023-07-19	9.8	Critical
CVE-2023-3519	citrix - multiple products	Unauthenticated remote code execution	2023-07-19	9.8	Critical
CVE-2022-28734	gnu - grub2	Out-of-bounds write when handling split HTTP headers; When handling split HTTP headers, GRUB2 HTTP code accidentally moves its internal data buffer point by one position. This can lead to a out-of-bound write further when parsing the HTTP request, writing a NULL byte past the buffer. It's conceivable that an attacker controlled set of packets can lead to corruption of the GRUB2's internal memory metadata.	2023-07-20	9.8	Critical
CVE-2023-38203	adobe - multiple products	Adobe ColdFusion versions 2018u17 (and earlier), 2021u7 (and earlier) and 2023u1 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.	2023-07-20	9.8	Critical
CVE-2023-38426	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.4. ksmbd has an out-of-bounds read in smb2_find_context_vals when create_context's name_len is larger than the tag length.	2023-07-18	9.1	Critical
CVE-2023-38428	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.4. fs/ksmbd/smb2pdu.c in ksmbd does not properly check the UserName value because it does not consider the address of security buffer, leading to an out-of-bounds read.	2023-07-18	9.1	Critical
CVE-2023-38430	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.9. ksmbd does not validate the SMB request protocol ID, leading to an out-of-bounds read.	2023-07-18	9.1	Critical
CVE-2023-38431	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.8. fs/smb/server/connection.c in ksmbd does not validate the relationship between the NetBIOS header's length field and the	2023-07-18	9.1	Critical

		SMB header sizes, via pdu_size in ksmbd_conn_handler_loop, leading to an out-of-bounds read.			
CVE-2023-38432	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.10. fs/smb/server/smb2misc.c in ksmbd does not validate the relationship between the command payload size and the RFC1002 length specification, leading to an out-of-bounds read.	2023-07-18	9.1	Critical
CVE-2023-21974	oracle - application_express	Vulnerability in the Application Express Team Calendar Plugin product of Oracle Application Express (component: User Account). Supported versions that are affected are Application Express Team Calendar Plugin: 18.2-22.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Application Express Team Calendar Plugin. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Application Express Team Calendar Plugin, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Application Express Team Calendar Plugin. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).	2023-07-18	9	Critical
CVE-2023-21975	oracle - application_express	Vulnerability in the Application Express Customers Plugin product of Oracle Application Express (component: User Account). Supported versions that are affected are Application Express Customers Plugin: 18.2-22.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Application Express Customers Plugin. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Application Express Customers Plugin, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Application Express Customers Plugin. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).	2023-07-18	9	Critical
CVE-2023-28767	zyxel - usg_2200-vpn_firmware	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled.	2023-07-17	8.8	High
CVE-2023-33011	zyxel - usg_2200-vpn_firmware	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled.	2023-07-17	8.8	High
CVE-2023-33012	zyxel - usg_20w-vpn_firmware	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	2023-07-17	8.8	High
CVE-2023-34139	zyxel - usg_2200-vpn_firmware	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device.	2023-07-17	8.8	High
CVE-2023-38404	veritas - infoscale_operations_manager	The XPRTLD web application in Veritas InfoScale Operations Manager (VIOM) before 8.0.0.410 allows an authenticated attacker to upload all types of files to the server. An authenticated attacker can then execute the malicious file to perform command execution on the remote server.	2023-07-17	8.8	High
CVE-2023-28754	apache - shardingsphere	Deserialization of Untrusted Data vulnerability in Apache ShardingSphere-Agent, which allows attackers to execute arbitrary code by constructing a special YAML configuration file. The attacker needs to have permission to modify the ShardingSphere Agent YAML configuration file on the target machine, and the target machine can access the URL with the	2023-07-19	8.8	High

		arbitrary code JAR. An attacker can use SnakeYAML to deserialize java.net.URLClassLoader and make it load a JAR from a specified URL, and then deserialize javax.script.ScriptEngineManager to load code using that ClassLoader. When the ShardingSphere JVM process starts and uses the ShardingSphere-Agent, the arbitrary code specified by the attacker will be executed during the deserialization of the YAML configuration file by the Agent. This issue affects ShardingSphere-Agent: through 5.3.2. This vulnerability is fixed in Apache ShardingSphere 5.4.0.			
CVE-2023-22062	oracle - hyperion	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Repository). The supported version that is affected is 11.2.13.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. While the vulnerability is in Oracle Hyperion Financial Reporting, 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 Hyperion Financial Reporting accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 8.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L).	2023-07-18	8.5	High
CVE-2023-22014	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2023-07-18	8.4	High
CVE-2023-22018	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via RDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2023-07-18	8.1	High
CVE-2022-28733	gnu - grub2	Integer underflow in grub_net_recv_ip4_packets; A malicious crafted IP packet can lead to an integer underflow in grub_net_recv_ip4_packets() function on rsm->total_len value. Under certain circumstances the total_len value may end up wrapping around to a small integer number which will be used in memory allocation. If the attack succeeds in such way, subsequent operations can write past the end of the buffer.	2023-07-20	8.1	High
CVE-2023-34138	zyxel - usg_20w-vpn_firmware	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance.	2023-07-17	8	High
CVE-2023-34141	zyxel - usg_20w-vpn_firmware	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance.	2023-07-17	8	High
CVE-2023-3467	citrix - multiple products	Privilege Escalation to root administrator (nsroot)	2023-07-19	8	High
CVE-2023-30988	ibm - multiple products	The IBM i 7.2, 7.3, 7.4, and 7.5 product Facsimile Support for i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can	2023-07-16	7.8	High

		elevate privileges to gain root access to the host operating system. IBM X-Force ID: 254016.			
CVE-2023-30989	ibm - multiple products	IBM Performance Tools for i 7.2, 7.3, 7.4, and 7.5 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain all object access to the host operating system. IBM X-Force ID: 254017.	2023-07-16	7.8	High
CVE-2023-22023	oracle - solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Device Driver Interface). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. Note: CVE-2023-22023 is equivalent to CVE-2023-31284. 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).	2023-07-18	7.8	High
CVE-2022-43910	ibm - security_guardium	IBM Security Guardium 11.3 could allow a local user to escalate their privileges due to improper permission controls. IBM X-Force ID: 240908.	2023-07-19	7.8	High
CVE-2022-28735	gnu - grub2	The GRUB2's shim_lock verifier allows non-kernel files to be loaded on shim-powered secure boot systems. Allowing such files to be loaded may lead to unverified code and modules to be loaded in GRUB2 breaking the secure boot trust-chain.	2023-07-20	7.8	High
CVE-2022-28736	gnu - grub2	There's a use-after-free vulnerability in grub_cmd_chainloader() function; The chainloader command is used to boot up operating systems that doesn't support multiboot and do not have direct support from GRUB2. When executing chainloader more than once a use-after-free vulnerability is triggered. If an attacker can control the GRUB2's memory allocation pattern sensitive data may be exposed and arbitrary code execution can be achieved.	2023-07-20	7.8	High
CVE-2022-28737	redhat - shim	There's a possible overflow in handle_image() when shim tries to load and execute crafted EFI executables; The handle_image() function takes into account the SizeOfRawData field from each section to be loaded. An attacker can leverage this to perform out-of-bound writes into memory. Arbitrary code execution is not discarded in such scenario.	2023-07-20	7.8	High
CVE-2021-39822	adobe - indesign	Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious BMP file.	2023-07-20	7.8	High
CVE-2023-22060	oracle - hyperion_workspace	Vulnerability in the Oracle Hyperion Workspace product of Oracle Hyperion (component: UI and Visualization). The supported version that is affected is 11.2.13.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Workspace. 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 Hyperion Workspace accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Workspace accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Workspace. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L).	2023-07-18	7.6	High
CVE-2023-30383	tp-link - archer_c2_v1_firmware	TP-LINK Archer C50v2 Archer C50(US)_V2_160801, TP-LINK Archer C20v1 Archer_C20_V1_150707, and TP-LINK Archer C2v1 Archer_C2_US__V1_170228 were discovered to contain a buffer overflow which may lead to a Denial of Service (DoS) when parsing crafted data.	2023-07-18	7.5	High
CVE-2023-22047	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks 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 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).	2023-07-18	7.5	High
CVE-2021-38933	ibm - sterling_connect\	IBM Sterling Connect:Direct for UNIX 1.5 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 210574.	2023-07-19	7.5	High
CVE-2023-26023	ibm - cloud_pak_for_data	Planning Analytics Cartridge for Cloud Pak for Data 4.0 exposes sensitive information in logs which could lead an attacker to exploit this vulnerability to conduct further attacks. IBM X-Force ID: 247896.	2023-07-19	7.5	High

CVE-2023-26026	ibm - cloud_pak_for_data	Planning Analytics Cartridge for Cloud Pak for Data 4.0 exposes sensitive information in logs which could lead an attacker to exploit this vulnerability to conduct further attacks. IBM X-Force ID: 247896.	2023-07-19	7.5	High
CVE-2023-27877	ibm - cloud_pak_for_data	IBM Planning Analytics Cartridge for Cloud Pak for Data 4.0 connects to a CouchDB server. An attacker can exploit an insecure password policy to the CouchDB server and collect sensitive information from the database. IBM X-Force ID: 247905.	2023-07-19	7.5	High
CVE-2022-2127	samba - multiple products	An out-of-bounds read vulnerability was found in Samba due to insufficient length checks in winbindd_pam_auth_crap.c. When performing NTLM authentication, the client replies to cryptographic challenges back to the server. These replies have variable lengths, and Winbind fails to check the lan manager response length. When Winbind is used for NTLM authentication, a maliciously crafted request can trigger an out-of-bounds read in Winbind, possibly resulting in a crash.	2023-07-20	7.5	High
CVE-2023-30799	mikrotik - multiple products	MikroTik RouterOS stable before 6.49.7 and long-term through 6.48.6 are vulnerable to a privilege escalation issue. A remote and authenticated attacker can escalate privileges from admin to super-admin on the Winbox or HTTP interface. The attacker can abuse this vulnerability to execute arbitrary code on the system.	2023-07-19	7.2	High
CVE-2023-35012	ibm - db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 with a Federated configuration is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user with SYSADM privileges could overflow the buffer and execute arbitrary code on the system. IBM X-Force ID: 257763.	2023-07-17	6.7	Medium
CVE-2021-43072	fortinet - multiple products	A buffer copy without checking size of input ('classic buffer overflow') in Fortinet FortiAnalyzer version 7.0.2 and below, version 6.4.7 and below, version 6.2.9 and below, version 6.0.11 and below, version 5.6.11 and below, FortiManager version 7.0.2 and below, version 6.4.7 and below, version 6.2.9 and below, version 6.0.11 and below, version 5.6.11 and below, FortiOS version 7.0.0 through 7.0.4, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x and FortiProxy version 7.0.0 through 7.0.3, 2.0.0 through 2.0.8, 1.2.x, 1.1.x and 1.0.x allows attacker to execute unauthorized code or commands via crafted CLI `execute restore image` and `execute certificate remote` operations with the tFTP protocol.	2023-07-18	6.7	Medium
CVE-2023-34140	zyxel - usg_20w-vpn_firmware	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon.	2023-07-17	6.5	Medium
CVE-2021-32256	gnu - binutils	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.	2023-07-18	6.5	Medium
CVE-2023-21994	oracle - fusion_middleware	Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2023-07-18	6.5	Medium
CVE-2023-22022	oracle - multiple products	Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2023-07-18	6.5	Medium
CVE-2023-22037	oracle - web_applications_desktop_integrator	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: MS Excel Specific). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with	2023-07-18	6.5	Medium

		network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Web Applications Desktop Integrator, 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 Web Applications Desktop Integrator accessible data as well as unauthorized read access to a subset of Oracle Web Applications Desktop Integrator accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Web Applications Desktop Integrator. 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).			
CVE-2023-22040	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).	2023-07-18	6.5	Medium
CVE-2023-35898	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information due to an insecure security configuration in InfoSphere Data Flow Designer. IBM X-Force ID: 259352.	2023-07-19	6.5	Medium
CVE-2022-43908	ibm - security_guardium	IBM Security Guardium 11.3 could allow an authenticated user to cause a denial of service due to improper input validation. IBM X-Force ID: 240903.	2023-07-19	6.5	Medium
CVE-2023-32261	microfocus - dimensions_cm	A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. See the following Jenkins security advisory for details: * https://www.jenkins.io/security/advisory/2023-06-14/ https://www.jenkins.io/security/advisory/2023-06-14/	2023-07-19	6.5	Medium
CVE-2023-32262	microfocus - dimensions_cm	A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability allows attackers with Item/Configure permission to access and capture credentials they are not entitled to. See the following Jenkins security advisory for details: * https://www.jenkins.io/security/advisory/2023-06-14/ https://www.jenkins.io/security/advisory/2023-06-14/	2023-07-19	6.5	Medium
CVE-2023-32481	dell - wyse_management_suite	Wyse Management Suite versions prior to 4.0 contain a denial-of-service vulnerability. An authenticated malicious user can flood the configured SMTP server with numerous requests in order to deny access to the system.	2023-07-20	6.5	Medium
CVE-2023-33231	solarwinds - database_performance_analyzer	XSS attack was possible in DPA 2023.2 due to insufficient input validation	2023-07-18	6.1	Medium
CVE-2023-22035	oracle - e-business_suite	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: iSurvey Module). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, 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 Scripting accessible data as well as unauthorized read access to a subset of Oracle Scripting 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).	2023-07-18	6.1	Medium

CVE-2023-22042	oracle - applications_framework	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.2.3-12.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, 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 Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework 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).	2023-07-18	6.1	Medium
CVE-2023-22055	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 9.2.7.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2023-07-18	6.1	Medium
CVE-2023-3466	citrix - multiple products	Reflected Cross-Site Scripting (XSS)	2023-07-19	6.1	Medium
CVE-2023-21961	oracle - hyperion_essbase_administration_services	Vulnerability in the Oracle Hyperion Essbase Administration Services product of Oracle Essbase (component: EAS Administration and EAS Console). The supported version that is affected is 21.4.3.0.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Essbase Administration Services executes to compromise Oracle Hyperion Essbase Administration Services. While the vulnerability is in Oracle Hyperion Essbase Administration 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 Hyperion Essbase Administration Services 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).	2023-07-18	6	Medium
CVE-2023-22043	oracle - multiple products	Vulnerability in Oracle Java SE (component: JavaFX). The supported version that is affected is Oracle Java SE: 8u371. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE 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 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	2023-07-18	5.9	Medium
CVE-2023-22053	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.42 and prior and 8.0.33 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H).	2023-07-18	5.9	Medium
CVE-2023-32263	microfocus - dimensions_cm	A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability could be exploited to retrieve a login certificate if an authenticated user is duped into using an attacker-controlled Dimensions CM server. This vulnerability only applies when the Jenkins plugin is configured to use login certificate credentials.	2023-07-19	5.7	Medium

		https://www.jenkins.io/security/advisory/2023-06-14/			
CVE-2023-21983	oracle - application_express	Vulnerability in the Application Express Administration product of Oracle Application Express (component: None). Supported versions that are affected are Application Express Administration: 18.2-22.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Application Express Administration. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Application Express Administration accessible data as well as unauthorized read access to a subset of Application Express Administration accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Application Express Administration. 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).	2023-07-18	5.6	Medium
CVE-2023-38409	linux - linux_kernel	An issue was discovered in set_con2fb_map in drivers/video/fbdev/core/fbcon.c in the Linux kernel before 6.2.12. Because an assignment occurs only for the first vc, the fbcon_registered_fb and fbcon_display arrays can be desynchronized in fbcon_mode_deleted (the con2fb_map points at the old fb_info).	2023-07-17	5.5	Medium
CVE-2023-0160	linux - linux_kernel	A deadlock flaw was found in the Linux kernel's BPF subsystem. This flaw allows a local user to potentially crash the system.	2023-07-18	5.5	Medium
CVE-2023-37139	microsoft - chakracore	ChakraCore branch master cbb9b was discovered to contain a stack overflow vulnerability via the function Js::ScopeSlots::IsDebuggerScopeSlotArray().	2023-07-18	5.5	Medium
CVE-2023-37140	microsoft - chakracore	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function Js::DiagScopeVariablesWalker::GetChildrenCount().	2023-07-18	5.5	Medium
CVE-2023-37141	microsoft - chakracore	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function Js::ProfilingHelpers::ProfiledNewScArray().	2023-07-18	5.5	Medium
CVE-2023-37142	microsoft - chakracore	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function Js::EntryPointInfo::HasInlinees().	2023-07-18	5.5	Medium
CVE-2023-37143	microsoft - chakracore	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function BackwardPass::IsEmptyLoopAfterMemOp().	2023-07-18	5.5	Medium
CVE-2023-22017	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Easily exploitable 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 ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2023-07-18	5.5	Medium
CVE-2023-32446	dell - wyse_thinos	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files.	2023-07-20	5.5	Medium
CVE-2023-32447	dell - wyse_thinos	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files.	2023-07-20	5.5	Medium
CVE-2023-32455	dell - wyse_thinos	Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files.	2023-07-20	5.5	Medium
CVE-2023-22011	oracle - multiple products	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. 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 update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).	2023-07-18	5.4	Medium

CVE-2023-22020	oracle - multiple products	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. 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 update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition 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).	2023-07-18	5.4	Medium
CVE-2023-22039	oracle - agile_plm	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: WebClient). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agile PLM, 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 Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM 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).	2023-07-18	5.4	Medium
CVE-2023-22050	oracle - jd_edwards_enterpriseone_orchestrator	Vulnerability in the JD Edwards EnterpriseOne Orchestrator product of Oracle JD Edwards (component: E1 IOT Orchestrator Security). Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Orchestrator accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Orchestrator 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).	2023-07-18	5.4	Medium
CVE-2023-22061	oracle - business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Visual Analyzer). 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 and while the vulnerability is in Oracle Business Intelligence 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 Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition 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).	2023-07-18	5.4	Medium
CVE-2023-30433	ibm - security_verify_access	IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186.	2023-07-19	5.4	Medium
CVE-2023-29260	ibm - sterling_connect\	IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135.	2023-07-19	5.4	Medium
CVE-2023-25929	ibm - multiple products	IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861.	2023-07-22	5.4	Medium
CVE-2023-28530	ibm - multiple products	IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials. IBM X-Force ID: 251214.	2023-07-22	5.4	Medium

CVE-2023-33857	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain system information using a specially crafted query that could aid in further attacks against the system. IBM X-Force ID: 257695.	2023-07-17	5.3	Medium
CVE-2023-35901	ibm - multiple products	IBM Robotic Process Automation 21.0.0 through 21.0.7.6 and 23.0.0 through 23.0.6 is vulnerable to client side validation bypass which could allow invalid changes or values in some fields. IBM X-Force ID: 259380.	2023-07-17	5.3	Medium
CVE-2023-34036	vmware - multiple products	Reactive web applications that use Spring HATEOAS to produce hypermedia-based responses might be exposed to malicious forwarded headers if they are not behind a trusted proxy that ensures correctness of such headers, or if they don't have anything else in place to handle (and possibly discard) forwarded headers either in WebFlux or at the level of the underlying HTTP server. For the application to be affected, it needs to satisfy the following requirements: * It needs to use the reactive web stack (Spring WebFlux) and Spring HATEOAS to create links in hypermedia-based responses. * The application infrastructure does not guard against clients submitting (X-)Forwarded… headers.	2023-07-17	5.3	Medium
CVE-2023-34035	vmware - multiple products	Spring Security versions 5.8 prior to 5.8.5, 6.0 prior to 6.0.5, and 6.1 prior to 6.1.2 could be susceptible to authorization rule misconfiguration if the application uses requestMatchers(String) and multiple servlets, one of them being Spring MVC's DispatcherServlet. (DispatcherServlet is a Spring MVC component that maps HTTP endpoints to methods on @Controller-annotated classes.) Specifically, an application is vulnerable when all of the following are true: * Spring MVC is on the classpath * Spring Security is securing more than one servlet in a single application (one of them being Spring MVC's DispatcherServlet) * The application uses requestMatchers(String) to refer to endpoints that are not Spring MVC endpoints An application is not vulnerable if any of the following is true: * The application does not have Spring MVC on the classpath * The application secures no servlets other than Spring MVC's DispatcherServlet * The application uses requestMatchers(String) only for Spring MVC endpoints	2023-07-18	5.3	Medium
CVE-2023-35900	ibm - multiple products	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to disclosing server version information which may be used to determine software vulnerabilities at the operating system level. IBM X-Force ID: 259368.	2023-07-19	5.3	Medium
CVE-2023-29259	ibm - sterling_connect\	IBM Sterling Connect:Express for UNIX 1.5 browser UI is vulnerable to attacks that rely on the use of cookies without the SameSite attribute. IBM X-Force ID: 252055.	2023-07-19	5.3	Medium
CVE-2023-3446	openssl - multiple products	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length.	2023-07-19	5.3	Medium

		However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.			
CVE-2023-22041	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. 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, Oracle GraalVM for JDK 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 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2023-07-18	5.1	Medium
CVE-2023-21950	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in 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).	2023-07-18	4.9	Medium
CVE-2023-22007	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.41 and prior and 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).	2023-07-18	4.9	Medium
CVE-2023-22008	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.33 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).	2023-07-18	4.9	Medium
CVE-2023-22034	oracle - multiple products	Vulnerability in the Unified Audit component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. Easily exploitable vulnerability allows high privileged attacker having SYSDBA privilege with network access via Oracle	2023-07-18	4.9	Medium

		Net to compromise Unified Audit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Unified Audit accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).			
CVE-2023-22046	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 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).	2023-07-18	4.9	Medium
CVE-2023-22054	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 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).	2023-07-18	4.9	Medium
CVE-2023-22056	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 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).	2023-07-18	4.9	Medium
CVE-2023-22057	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.33 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).	2023-07-18	4.9	Medium
CVE-2023-32482	dell - wyse_management_suite	Wyse Management Suite versions prior to 4.0 contain an improper authorization vulnerability. An authenticated malicious user with privileged access can push policies to unauthorized tenant group.	2023-07-20	4.9	Medium
CVE-2023-33832	ibm - multiple products	IBM Spectrum Protect 8.1.0.0 through 8.1.17.0 could allow a local user to cause a denial of service due to due to improper time-of-check to time-of-use functionality. IBM X-Force ID: 256012.	2023-07-19	4.7	Medium
CVE-2023-22005	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.33 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).	2023-07-18	4.4	Medium
CVE-2023-22031	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 14.1.1.0.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic 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).	2023-07-18	4.4	Medium
CVE-2023-22033	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.33 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).	2023-07-18	4.4	Medium
CVE-2023-22058	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows high	2023-07-18	4.4	Medium

		privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).			
CVE-2023-32483	dell - wyse_management_suite	Wyse Management Suite versions prior to 4.0 contain a sensitive information disclosure vulnerability. An authenticated malicious user having local access to the system running the application could exploit this vulnerability to read sensitive information written to log files.	2023-07-20	4.4	Medium
CVE-2023-22004	oracle - e-business_suite	Vulnerability in the Oracle Applications Technology product of Oracle E-Business Suite (component: Reports Configuration). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Technology. 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 Applications Technology accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	2023-07-18	4.3	Medium
CVE-2023-22009	oracle - self-service_human_resources	Vulnerability in the Oracle Self-Service Human Resources product of Oracle E-Business Suite (component: Workforce Management). 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 Self-Service Human Resources. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Self-Service Human Resources 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).	2023-07-18	4.3	Medium
CVE-2023-22012	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 7.0.0.0.0. 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 update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2023-07-18	4.3	Medium
CVE-2023-22013	oracle - multiple products	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. 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 update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2023-07-18	4.3	Medium
CVE-2023-22021	oracle - multiple products	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. 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 ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2023-07-18	4.3	Medium
CVE-2023-22027	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 7.0.0.0.0. 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 ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2023-07-18	4.3	Medium
CVE-2023-22016	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker.	2023-07-18	4.2	Medium

		Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H).			
CVE-2023-21949	oracle - multiple products	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Advanced Networking Option accessible data. 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).	2023-07-18	3.7	Low
CVE-2023-22036	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also 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. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	2023-07-18	3.7	Low
CVE-2023-22044	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also 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. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	3.7	Low
CVE-2023-22045	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also 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. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	3.7	Low
CVE-2023-22049	debian - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit	2023-07-18	3.7	Low

		vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also 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. 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-2023-22051	oracle - multiple products	Vulnerability in the Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: GraalVM Compiler). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	3.7	Low
CVE-2023-22006	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. 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 Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK 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 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	2023-07-18	3.1	Low
CVE-2023-22048	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	3.1	Low
CVE-2023-22052	oracle - multiple products	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	2023-07-18	3.1	Low
CVE-2023-22038	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2023-07-18	2.7	Low
CVE-2023-22010	oracle - essbase	Vulnerability in Oracle Essbase (component: Security and Provisioning). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N).	2023-07-18	2.2	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.