الهيئة الوطنية للأمن السيبراني
National 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 October to 21st of October. 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 اكتوبر إلى ٢١ اكتوبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدًا: 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-2023-20198	cisco - ios_xe	Cisco is aware of active exploitation of a previously unknown vulnerability in the web UI feature of Cisco IOS XE Software when exposed to the internet or to untrusted networks. This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access. The attacker can then use that account to gain control of the affected system. For steps to close the attack vector for this vulnerability, see the Recommendations section of this advisory Cisco will provide updates on the status of this investigation and when a software patch is available.	2023-10-16	10	Critical
CVE-2023-45871	linux - linux_kernel	An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel before 6.5.3. A buffer size may not be adequate for frames larger than the MTU.	2023-10-15	9.8	Critical
CVE-2023-33836	ibm - security_verify_governance	IBM Security Verify Governance 10.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 256016.	2023-10-16	9.8	Critical
CVE-2023-43668	apache - inlong	Authorization Bypass Through User-Controlled Key vulnerability in Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.8.0, some sensitive params checks will be bypassed, like "autoDeserizalize","allowLoadLocalInfile".... . Users are advised to upgrade to Apache InLong's 1.9.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/8604	2023-10-16	9.8	Critical
CVE-2023-22069	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 unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2023-10-17	9.8	Critical
CVE-2023-22072	oracle - weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). The supported version	2023-10-17	9.8	Critical

		that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
CVE-2023-22089	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 unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2023-10-17	9.8	Critical
CVE-2023-35084	ivanti - multiple products	Unsafe Deserialization of User Input could lead to Execution of Unauthorized Operations in Ivanti Endpoint Manager 2022 su3 and all previous versions, which could allow an attacker to execute commands remotely.	2023-10-18	9.8	Critical
CVE-2023-35182	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability can be abused by unauthenticated users on SolarWinds ARM Server.	2023-10-19	9.8	Critical
CVE-2023-35184	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an unauthenticated user to abuse a SolarWinds service resulting in a remote code execution.	2023-10-19	9.8	Critical
CVE-2023-35187	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal Remote Code Vulnerability. This vulnerability allows an unauthenticated user to achieve the Remote Code Execution.	2023-10-19	9.8	Critical
CVE-2023-40791	linux - linux_kernel	extract_user_to_sg in lib/scatterlist.c in the Linux kernel before 6.4.12 fails to unpin pages in a certain situation, as demonstrated by a WARNING for try_grab_page.	2023-10-16	9.1	Critical
CVE-2022-22375	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 221681.	2023-10-17	8.8	High
CVE-2023-22085	oracle - hospitality_opera_5_property_services	Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (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:H).	2023-10-17	8.8	High
CVE-2023-22087	oracle - hospitality_opera_5_property_services	Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (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:H).	2023-10-17	8.8	High
CVE-2023-41715	sonicwall - sonicos	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel.	2023-10-17	8.8	High
CVE-2023-35180	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API.	2023-10-19	8.8	High
CVE-2023-35186	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution.	2023-10-19	8.8	High
CVE-2023-23373	qnap - qusbcam2	An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: QUSBCam2 2.0.3 (2023/06/15) and later	2023-10-20	8.8	High
CVE-2023-22102	oracle - mysql	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.1.0 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker	2023-10-17	8.3	High

		and while the vulnerability is in MySQL Connectors, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).			
CVE-2023-22101	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. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. 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).	2023-10-17	8.1	High
CVE-2023-22094	oracle - mysql_installer	Vulnerability in the MySQL Installer product of Oracle MySQL (component: Installer: General). Supported versions that are affected are Prior to 1.6.8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Installer executes to compromise MySQL Installer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Installer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Installer accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Installer. Note: This patch is used in MySQL Server bundled version 8.0.35 and 5.7.44. CVSS 3.1 Base Score 7.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:H).	2023-10-17	7.9	High
CVE-2023-22100	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12. 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 and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:H).	2023-10-17	7.9	High
CVE-2023-40378	ibm - multiple products	IBM Directory Server for IBM i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263584.	2023-10-15	7.8	High
CVE-2023-40377	ibm - multiple products	Backup, Recovery, and Media Services (BRMS) for IBM i 7.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263583.	2023-10-16	7.8	High
CVE-2023-38280	ibm - multiple products	IBM HMC (Hardware Management Console) 10.1.1010.0 and 10.2.1030.0 could allow a local user to escalate their privileges to root access on a restricted shell. IBM X-Force ID: 260740.	2023-10-16	7.8	High
CVE-2023-45898	linux - linux_kernel	The Linux kernel before 6.5.4 has an es1 use-after-free in fs/ext4/extents_status.c, related to ext4_es_insert_extent.	2023-10-16	7.8	High
CVE-2023-35181	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows users to abuse incorrect folder permission resulting in Privilege Escalation.	2023-10-19	7.8	High
CVE-2023-35183	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation.	2023-10-19	7.8	High
CVE-2023-34045	vmware - fusion	VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed or being installed for the first time.	2023-10-20	7.8	High
CVE-2023-43667	apache - inlong	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.8.0, the attacker	2023-10-16	7.5	High

		can create misleading or false records, making it harder to audit and trace malicious activities. Users are advised to upgrade to Apache InLong's 1.8.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/8628			
CVE-2023-4457	grafana - google_sheets	Grafana is an open-source platform for monitoring and observability. The Google Sheets data source plugin for Grafana, versions 0.9.0 to 1.2.2 are vulnerable to an information disclosure vulnerability. The plugin did not properly sanitize error messages, making it potentially expose the Google Sheet API-key that is configured for the data source. This vulnerability was fixed in version 1.2.2.	2023-10-16	7.5	High
CVE-2023-30987	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain databases. IBM X-Force ID: 253440.	2023-10-16	7.5	High
CVE-2023-38720	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 and 11.5 is vulnerable to denial of service with a specially crafted ALTER TABLE statement. IBM X-Force ID: 261616.	2023-10-16	7.5	High
CVE-2023-38728	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted XML query statement. IBM X-Force ID: 262258.	2023-10-16	7.5	High
CVE-2023-38740	ibm - db2	IBM Db2 for Linux, UNIX, and Windows (includes Db2 Connect Server) 11.5 is vulnerable to a denial of service with a specially crafted SQL statement. IBM X-Force ID: 262613.	2023-10-16	7.5	High
CVE-2023-30991	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 254037.	2023-10-16	7.5	High
CVE-2023-40374	ibm - db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service with a specially crafted query statement. IBM X-Force ID: 263575.	2023-10-16	7.5	High
CVE-2023-40372	ibm - db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service with a specially crafted SQL statement using External Tables. IBM X-Force ID: 263499.	2023-10-17	7.5	High
CVE-2023-40373	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to denial of service with a specially crafted query containing common table expressions. IBM X-Force ID: 263574.	2023-10-17	7.5	High
CVE-2022-22385	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could disclose sensitive information to an attacked due to the transmission of data in clear text. IBM X-Force ID: 221962.	2023-10-17	7.5	High
CVE-2023-39456	apache - traffic_server	Improper Input Validation vulnerability in Apache Traffic Server with malformed HTTP/2 frames.This issue affects Apache Traffic Server: from 9.0.0 through 9.2.2. Users are recommended to upgrade to version 9.2.3, which fixes the issue.	2023-10-17	7.5	High
CVE-2023-41752	apache - multiple products	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Traffic Server.This issue affects Apache Traffic Server: from 8.0.0 through 8.1.8, from 9.0.0 through 9.2.2. Users are recommended to upgrade to version 8.1.9 or 9.2.3, which fixes the issue.	2023-10-17	7.5	High
CVE-2023-22019	oracle - http_server	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HTTP 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).	2023-10-17	7.5	High
CVE-2023-22086	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 unauthenticated attacker with network access via T3, IIOP 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).	2023-10-17	7.5	High

CVE-2023-22108	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 unauthenticated attacker with network access via T3, IIOP 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).	2023-10-17	7.5	High
CVE-2023-41713	sonicwall - sonicos	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function.	2023-10-17	7.5	High
CVE-2023-5552	sophos - firewall	A password disclosure vulnerability in the Secure PDF eXchange (SPX) feature allows attackers with full email access to decrypt PDFs in Sophos Firewall version 19.5 MR3 (19.5.3) and older, if the password type is set to “Specified by sender”.	2023-10-18	7.5	High
CVE-2023-35656	google - android	In multiple functions of protocolembmsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-18	7.5	High
CVE-2023-35663	google - android	In Init of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-18	7.5	High
CVE-2023-46227	apache - inlong	Deserialization of Untrusted Data Vulnerability in Apache Software Foundation Apache InLong. This issue affects Apache InLong: from 1.4.0 through 1.8.0, the attacker can use \t to bypass. Users are advised to upgrade to Apache InLong's 1.9.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/8814	2023-10-19	7.5	High
CVE-2023-22098	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H).	2023-10-17	7.3	High
CVE-2023-22099	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H).	2023-10-17	7.3	High
CVE-2023-35018	ibm - security_verify_governance	IBM Security Verify Governance 10.0 could allow a privileged use to upload arbitrary files due to improper file validation. IBM X-Force ID: 259382.	2023-10-16	7.2	High
CVE-2023-4822	grafana - multiple products	Grafana is an open-source platform for monitoring and observability. The vulnerability impacts Grafana instances with several organizations, and allows a user with Organization Admin permissions in one organization to change the permissions associated with Organization Viewer, Organization Editor and Organization Admin roles in all organizations.	2023-10-16	7.2	High

		It also allows an Organization Admin to assign or revoke any permissions that they have to any user globally. This means that any Organization Admin can elevate their own permissions in any organization that they are already a member of, or elevate or restrict the permissions of any other user. The vulnerability does not allow a user to become a member of an organization that they are not already a member of, or to add any other users to an organization that the current user is not a member of.			
CVE-2023-4399	grafana - multiple products	Grafana is an open-source platform for monitoring and observability. In Grafana Enterprise, Request security is a deny list that allows admins to configure Grafana in a way so that the instance doesn't call specific hosts. However, the restriction can be bypassed used punycode encoding of the characters in the request address.	2023-10-17	7.2	High
CVE-2023-35185	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal Remote Code Vulnerability using SYSTEM privileges.	2023-10-19	7.2	High
CVE-2021-29913	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premise 11.5 could allow an authenticated user to obtain sensitive information or perform unauthorized actions due to improper input validation. IBM X-Force ID: 207898.	2023-10-17	7.1	High
CVE-2023-34046	vmware - fusion	VMware Fusion(13.x prior to 13.5) contains a TOCTOU (Time-of-check Time-of-use) vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed or being installed for the first time.	2023-10-20	7	High
CVE-2023-43666	apache - inlong	Insufficient Verification of Data Authenticity vulnerability in Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.8.0, General user can view all user data like Admin account. Users are advised to upgrade to Apache InLong's 1.9.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/8623	2023-10-16	6.5	Medium
CVE-2023-4896	arubanetworks - multiple products	A vulnerability exists which allows an authenticated attacker to access sensitive information on the AirWave Management Platform web-based management interface. Successful exploitation allows the attacker to gain access to some data that could be further exploited to laterally access devices managed and monitored by the AirWave server.	2023-10-17	6.5	Medium
CVE-2023-22059	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. 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).	2023-10-17	6.5	Medium
CVE-2023-22079	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 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).	2023-10-17	6.5	Medium
CVE-2023-22090	oracle - peoplesoft_enterprise_cost_center_common_application_objects	Vulnerability in the PeopleSoft Enterprise CC Common Application Objects product of Oracle PeopleSoft (component: Events & Notifications). 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 CC Common Application Objects. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CC Common	2023-10-17	6.5	Medium

		Application Objects 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-2023-22093	oracle - e-business_suite	Vulnerability in the Oracle iRecruitment product of Oracle E-Business Suite (component: Requisition and Vacancy). 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 iRecruitment. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iRecruitment accessible data as well as unauthorized read access to a subset of Oracle iRecruitment accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2023-10-17	6.5	Medium
CVE-2023-22095	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). The supported version that is affected is 8.1.0. 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).	2023-10-17	6.5	Medium
CVE-2023-22106	oracle - multiple products	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: API). Supported versions that are affected are ECC: 8, 9 and 10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2023-10-17	6.5	Medium
CVE-2023-22118	oracle - multiple products	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, 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 FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 6.5 (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).	2023-10-17	6.5	Medium
CVE-2023-39276	sonicwall - sonicos	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash.	2023-10-17	6.5	Medium
CVE-2023-39277	sonicwall - sonicos	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	2023-10-17	6.5	Medium
CVE-2023-39278	sonicwall - sonicos	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash.	2023-10-17	6.5	Medium
CVE-2023-39279	sonicwall - sonicos	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash.	2023-10-17	6.5	Medium
CVE-2023-39280	sonicwall - sonicos	SonicOS p ost-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash.	2023-10-17	6.5	Medium
CVE-2023-41711	sonicwall - sonicos	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash.	2023-10-17	6.5	Medium
CVE-2023-41712	sonicwall - sonicos	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash.	2023-10-17	6.5	Medium
CVE-2023-35083	ivanti - multiple products	Allows an authenticated attacker with network access to read arbitrary files on Endpoint Manager recently discovered on 2022	2023-10-18	6.5	Medium

		SU3 and all previous versions potentially leading to the leakage of sensitive information.			
CVE-2023-20261	cisco - multiple products	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user.	2023-10-18	6.5	Medium
CVE-2023-25753	apache - shenyu	There exists an SSRF (Server-Side Request Forgery) vulnerability located at the /sandbox/proxyGateway endpoint. This vulnerability allows us to manipulate arbitrary requests and retrieve corresponding responses by inputting any URL into the requestUrl parameter. Of particular concern is our ability to exert control over the HTTP method, cookies, IP address, and headers. This effectively grants us the capability to dispatch complete HTTP requests to hosts of our choosing. This issue affects Apache ShenYu: 2.5.1. Upgrade to Apache ShenYu 2.6.0 or apply patch https://github.com/apache/shenyu/pull/4776 .	2023-10-19	6.5	Medium
CVE-2023-44483	apache - multiple products	All versions of Apache Santuario - XML Security for Java prior to 2.2.6, 2.3.4, and 3.0.3, when using the JSR 105 API, are vulnerable to an issue where a private key may be disclosed in log files when generating an XML Signature and logging with debug level is enabled. Users are recommended to upgrade to version 2.2.6, 2.3.4, or 3.0.3, which fixes this issue.	2023-10-20	6.5	Medium
CVE-2023-22127	oracle - outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Content Access SDK, Image Export SDK, PDF Export SDK, HTML Export SDK). The supported version that is affected is 8.5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	2023-10-17	6.3	Medium
CVE-2023-45757	apache - brpc	Security vulnerability in Apache bRPC <=1.6.0 on all platforms allows attackers to inject XSS code to the builtin rpcz page. An attacker that can send http request to bRPC server with rpcz enabled can inject arbitrary XSS code to the builtin rpcz page. Solution (choose one of three): 1. upgrade to bRPC > 1.6.0, download link: https://dist.apache.org/repos/dist/release/brpc/1.6.1/ 2. If you are using an old version of bRPC and hard to upgrade, you can apply this patch: https://github.com/apache/brpc/pull/2411 3. disable rpcz feature	2023-10-16	6.1	Medium
CVE-2023-42497	liferay - multiple products	Reflected cross-site scripting (XSS) vulnerability on the Export for Translation page in Liferay Portal 7.4.3.4 through 7.4.3.85, and Liferay DXP 7.4 before update 86 allows remote attackers to inject arbitrary web script or HTML via the `_com_liferay_translation_web_internal_portlet_TranslationPortlet_redirect` parameter.	2023-10-17	6.1	Medium
CVE-2023-44311	liferay - multiple products	Multiple reflected cross-site scripting (XSS) vulnerabilities in the Plugin for OAuth 2.0 module's OAuth2ProviderApplicationRedirect class in Liferay Portal 7.4.3.41 through 7.4.3.89, and Liferay DXP 7.4 update 41 through update 89 allow remote attackers to inject arbitrary web script or HTML via the (1) code, or (2) error parameter. This issue is caused by an incomplete fix in CVE-2023-33941.	2023-10-17	6.1	Medium
CVE-2023-22029	oracle - commerce_guided_search	Vulnerability in the Oracle Commerce Guided Search product of Oracle Commerce (component: Workbench). The supported version that is affected is 11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search. Successful attacks require human interaction from a person other than the attacker	2023-10-17	6.1	Medium

		and while the vulnerability is in Oracle Commerce Guided Search, 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 Commerce Guided Search accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).			
CVE-2023-22076	oracle - e-business_suite	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Personalization). 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 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).	2023-10-17	6.1	Medium
CVE-2023-22080	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2023-10-17	6.1	Medium
CVE-2023-22107	oracle - multiple products	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: UI Components). Supported versions that are affected are ECC: 8, 9 and 10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Command Center 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 Enterprise Command Center Framework accessible data as well as unauthorized read access to a subset of Oracle Enterprise Command Center 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).	2023-10-17	6.1	Medium
CVE-2023-34044	vmware - workstation	VMware Workstation(17.x prior to 17.5) and Fusion(13.x prior to 13.5) contain an out-of-bounds read vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine. A malicious actor with local administrative privileges on a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine.	2023-10-20	6	Medium
CVE-2022-22386	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 221963.	2023-10-17	5.9	Medium
CVE-2023-22071	oracle - multiple products	Vulnerability in the PL/SQL component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having Create Session, Execute on sys.utl_http privilege with network access via Oracle Net to compromise PL/SQL. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PL/SQL, 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 PL/SQL accessible data as well as unauthorized read access to a subset of PL/SQL	2023-10-17	5.9	Medium

		accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PL/SQL. 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-2023-22119	oracle - multiple products	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L).	2023-10-17	5.9	Medium
CVE-2023-22122	oracle - banking_trade_finance	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Trade Finance accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Trade Finance accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Trade Finance. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L).	2023-10-17	5.9	Medium
CVE-2023-22130	oracle - sun_zfs_storage_appliance_kit	Vulnerability in the Sun ZFS Storage Appliance product of Oracle Systems (component: Core). The supported version that is affected is 8.8.60. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Sun ZFS Storage Appliance. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Sun ZFS Storage Appliance. 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).	2023-10-17	5.9	Medium
CVE-2023-22129	oracle - solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. Note: This vunlerability only affects SPARC Systems. 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).	2023-10-17	5.5	Medium
CVE-2023-42629	liferay - multiple products	Stored cross-site scripting (XSS) vulnerability in the manage vocabulary page in Liferay Portal 7.4.2 through 7.4.3.87, and Liferay DXP 7.4 before update 88 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a Vocabulary's 'description' text field.	2023-10-17	5.4	Medium
CVE-2023-44309	liferay - multiple products	Multiple stored cross-site scripting (XSS) vulnerabilities in the fragment components in Liferay Portal 7.4.2 through 7.4.3.53, and Liferay DXP 7.4 before update 54 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into any non-HTML field of a linked source asset.	2023-10-17	5.4	Medium
CVE-2023-44310	liferay - multiple products	Stored cross-site scripting (XSS) vulnerability in Page Tree menu Liferay Portal 7.3.6 through 7.4.3.78, and Liferay DXP 7.3 fix pack 1 through update 23, and 7.4 before update 79 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into page's "Name" text field.	2023-10-17	5.4	Medium
CVE-2023-42628	liferay - multiple products	Stored cross-site scripting (XSS) vulnerability in the Wiki widget in Liferay Portal 7.1.0 through 7.4.3.87, and Liferay DXP 7.0 fix pack 83 through 102, 7.1 fix pack 28 and earlier, 7.2 fix pack 20 and earlier, 7.3 update 33 and earlier, and 7.4 before update 88 allows remote attackers to inject arbitrary web script or HTML into a parent wiki page via a crafted payload injected into a wiki page's ‘Content’ text field.	2023-10-17	5.4	Medium
CVE-2023-42627	liferay - multiple products	Multiple stored cross-site scripting (XSS) vulnerabilities in the Commerce module in Liferay Portal 7.3.5 through 7.4.3.91, and Liferay DXP 7.3 update 33 and earlier, and 7.4 before update 92 allow remote attackers to inject arbitrary web script or HTML via a	2023-10-17	5.4	Medium

		crafted payload injected into a (1) Shipping Name, (2) Shipping Phone Number, (3) Shipping Address, (4) Shipping Address 2, (5) Shipping Address 3, (6) Shipping Zip, (7) Shipping City, (8) Shipping Region (9), Shipping Country, (10) Billing Name, (11) Billing Phone Number, (12) Billing Address, (13) Billing Address 2, (14) Billing Address 3, (15) Billing Zip, (16) Billing City, (17) Billing Region, (18) Billing Country, or (19) Region Code.			
CVE-2023-22082	oracle - multiple products	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Pod Admin). 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 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).	2023-10-17	5.4	Medium
CVE-2023-22105	oracle - multiple products	Vulnerability in the BI Publisher product of Oracle Analytics (component: Web 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 BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, 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 BI Publisher accessible data as well as unauthorized read access to a subset of BI Publisher 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).	2023-10-17	5.4	Medium
CVE-2023-22117	oracle - multiple products	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, 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 FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking 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).	2023-10-17	5.4	Medium
CVE-2023-22121	oracle - banking_trade_finance	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	2023-10-17	5.4	Medium
CVE-2023-22123	oracle - banking_trade_finance	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Trade Finance, 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 Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance 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).	2023-10-17	5.4	Medium

CVE-2023-22124	oracle - banking_trade_finance	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Trade Finance, 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 Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance 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).	2023-10-17	5.4	Medium
CVE-2023-22125	oracle - banking_trade_finance	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Trade Finance, 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 Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance 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).	2023-10-17	5.4	Medium
CVE-2023-5561	wordpress - multiple products	The Popup Builder WordPress plugin through 4.1.15 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	2023-10-16	5.3	Medium
CVE-2022-22377	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 221827.	2023-10-17	5.3	Medium
CVE-2021-38859	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a user to obtain version number information using a specially crafted HTTP request that could be used in further attacks against the system. IBM X-Force ID: 207899.	2023-10-17	5.3	Medium
CVE-2022-43889	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could disclose sensitive information through an HTTP request that could aid an attacker in further attacks against the system. IBM X-Force ID: 240452.	2023-10-17	5.3	Medium
CVE-2022-43891	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 240454.	2023-10-17	5.3	Medium
CVE-2022-43892	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 does not validate, or incorrectly validates, a certificate which could disclose sensitive information which could aid further attacks against the system. IBM X-Force ID: 240455.	2023-10-17	5.3	Medium
CVE-2023-22067	oracle - multiple products	Vulnerability in Oracle Java SE (component: CORBA). Supported versions that are affected are Oracle Java SE: 8u381 and 8u381-perf. Easily exploitable vulnerability allows unauthenticated attacker with network access via CORBA to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. 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).	2023-10-17	5.3	Medium
CVE-2023-22081	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8 and 21. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK.	2023-10-17	5.3	Medium

		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 for JDK. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).			
CVE-2023-22126	oracle - webcenter_content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Content 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).	2023-10-17	5.3	Medium
CVE-2023-22015	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 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 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).	2023-10-17	4.9	Medium
CVE-2023-22026	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 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 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).	2023-10-17	4.9	Medium
CVE-2023-22028	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.43 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 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).	2023-10-17	4.9	Medium
CVE-2023-22032	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. 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).	2023-10-17	4.9	Medium
CVE-2023-22064	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 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).	2023-10-17	4.9	Medium
CVE-2023-22065	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).	2023-10-17	4.9	Medium
CVE-2023-22066	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows	2023-10-17	4.9	Medium

		high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			
CVE-2023-22068	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. 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).	2023-10-17	4.9	Medium
CVE-2023-22070	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. 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).	2023-10-17	4.9	Medium
CVE-2023-22077	oracle - multiple products	Vulnerability in the Oracle Database Recovery Manager component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having DBA account privilege with network access via Oracle Net to compromise Oracle Database Recovery Manager. 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 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).	2023-10-17	4.9	Medium
CVE-2023-22078	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. 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).	2023-10-17	4.9	Medium
CVE-2023-22084	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.43 and prior, 8.0.34 and prior and 8.1.0. 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).	2023-10-17	4.9	Medium
CVE-2023-22092	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 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).	2023-10-17	4.9	Medium
CVE-2023-22097	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. 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).	2023-10-17	4.9	Medium
CVE-2023-22103	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. 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).	2023-10-17	4.9	Medium

CVE-2023-22104	oracle - mysql	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).	2023-10-17	4.9	Medium
CVE-2023-22110	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).	2023-10-17	4.9	Medium
CVE-2023-22111	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). 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).	2023-10-17	4.9	Medium
CVE-2023-22112	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 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).	2023-10-17	4.9	Medium
CVE-2023-22114	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. 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).	2023-10-17	4.9	Medium
CVE-2023-22115	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). 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).	2023-10-17	4.9	Medium
CVE-2023-22091	oracle - multiple products	Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8 and 21. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK accessible data as well as unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	2023-10-17	4.8	Medium
CVE-2023-22109	oracle - multiple products	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 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 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 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 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).	2023-10-17	4.6	Medium

CVE-2023-35013	ibm - security_verify_governance	IBM Security Verify Governance 10.0, Identity Manager could allow a local privileged user to obtain sensitive information from source code. IBM X-Force ID: 257769.	2023-10-16	4.4	Medium
CVE-2023-38719	ibm - db2	IBM Db2 11.5 could allow a local user with special privileges to cause a denial of service during database deactivation on DPF. IBM X-Force ID: 261607.	2023-10-17	4.4	Medium
CVE-2022-43893	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a privileged user to cause by using a malicious payload. IBM X-Force ID: 240634.	2023-10-17	4.4	Medium
CVE-2022-22384	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow an attacker to modify messages returned from the server due to hazardous input validation. IBM X-Force ID: 221961.	2023-10-17	4.3	Medium
CVE-2021-20581	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow a user to obtain sensitive information due to insufficient session expiration. IBM X-Force ID: 199324.	2023-10-17	4.3	Medium
CVE-2022-22380	ibm - security_verify_privilege_on-premises	IBM Security Verify Privilege On-Premises 11.5 could allow an attacker to spoof a trusted entity due to improperly validating certificates. IBM X-Force ID: 221957.	2023-10-17	4.3	Medium
CVE-2023-22073	oracle - multiple products	Vulnerability in the Oracle Notification Server component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Notification Server executes to compromise Oracle Notification Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Notification Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2023-10-17	4.3	Medium
CVE-2023-22083	oracle - enterprise_session_border_controller	Vulnerability in the Oracle Enterprise Session Border Controller product of Oracle Communications (component: Web UI). Supported versions that are affected are 9.0-9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Enterprise Session Border Controller. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Enterprise Session Border Controller accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N).	2023-10-17	4.3	Medium
CVE-2023-22088	oracle - multiple products	Vulnerability in the Oracle Communications Order and Service Management product of Oracle Communications Applications (component: User Management). Supported versions that are affected are 7.4.0 and 7.4.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Order and Service Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Order and Service 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).	2023-10-17	4.3	Medium
CVE-2023-22096	oracle - multiple products	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM 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).	2023-10-17	4.3	Medium
CVE-2023-34050	vmware - multiple products	In spring AMQP versions 1.0.0 to 2.4.16 and 3.0.0 to 3.0.9 , allowed list patterns for deserializable class names were added to Spring AMQP, allowing users to lock down deserialization of	2023-10-19	4.3	Medium

		data in messages from untrusted sources; however by default, when no allowed list was provided, all classes could be deserialized. Specifically, an application is vulnerable if * the SimpleMessageConverter or SerializerMessageConverter is used * the user does not configure allowed list patterns * untrusted message originators gain permissions to write messages to the RabbitMQ broker to send malicious content			
CVE-2023-22025	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: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8 and 21. 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 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).	2023-10-17	3.7	Low
CVE-2023-22128	oracle - multiple products	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via rquota to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	2023-10-17	3.1	Low
CVE-2023-22113	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2023-10-17	2.7	Low
CVE-2023-22074	oracle - multiple products	Vulnerability in the Oracle Database Sharding component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having Create Session, Select Any Dictionary privilege with network access via Oracle Net to compromise Oracle Database Sharding. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Database Sharding. CVSS 3.1 Base Score 2.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:L).	2023-10-17	2.4	Low

CVE-2023-22075	oracle - multiple products	Vulnerability in the Oracle Database Sharding component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having Create Session, Create Any View, Select Any Table privilege with network access via Oracle Net to compromise Oracle Database Sharding. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Database Sharding. CVSS 3.1 Base Score 2.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:L).	2023-10-17	2.4	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.