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 ١٤ يناير إلى ٢٠ يناير. 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 14th of January to 20th of January. 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-2023-46226	apache - iotdb	Remote Code Execution vulnerability in Apache IoTDB.This issue affects Apache IoTDB: from 1.0.0 through 1.2.2. Users are recommended to upgrade to version 1.3.0, which fixes the issue.	2024-01-15	9.8	Critical
CVE-2023-22527	atlassian - multiple products	A template injection vulnerability on older versions of Confluence Data Center and Server allows an unauthenticated attacker to achieve RCE on an affected instance. Customers using an affected version must take immediate action. Most recent supported versions of Confluence Data Center and Server are not affected by this vulnerability as it was ultimately mitigated during regular version updates. However, Atlassian recommends that customers take care to install the latest version to protect their instances from non-critical vulnerabilities outlined in Atlassian's January Security Bulletin.	2024-01-16	9.8	Critical
CVE-2023-52103	huawei - multiple products	Buffer overflow vulnerability in the FLP module. Successful exploitation of this vulnerability may cause out-of-bounds read.	2024-01-16	9.8	Critical
CVE-2024-20272	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system. This vulnerability is due to a lack of authentication in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by uploading arbitrary files to an affected system. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root.	2024-01-17	9.8	Critical
CVE-2023-52101	huawei - multiple products	Component exposure vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service availability and integrity.	2024-01-16	9.1	Critical
CVE-2023-52106	huawei - harmonyos	The DownloadProviderMain module has a vulnerability in API permission verification. Successful exploitation of this vulnerability may affect integrity and availability.	2024-01-16	9.1	Critical
CVE-2024-22317	ibm - multiple products	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.24 and 12.0.1.0 through 12.0.11.0 could allow a remote attacker to obtain sensitive information or cause a denial of service due to improper restriction of excessive authentication attempts. IBM X-Force ID: 279143.	2024-01-18	9.1	Critical
CVE-2024-0565	linux - multiple products	An out-of-bounds memory read flaw was found in receive_encrypted_standard in fs/smb/client/smb2ops.c in the SMB Client sub-component in the Linux Kernel. This issue occurs due to integer underflow on the memcpy length, leading to a denial of service.	2024-01-15	8.8	High
CVE-2023-22526	atlassian - multiple products	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 7.19.0 of Confluence Data Center.	2024-01-16	8.8	High

		This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.2, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Confluence Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Confluence Data Center and Server 7.19: Upgrade to a release 7.19.17, or any higher 7.19.x release Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html]). You can download the latest version of Confluence Data Center from the download center ([https://www.atlassian.com/software/confluence/download-archives]). This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program			
CVE-2024-21672	atlassian - multiple products	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 2.1.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.3 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H allows an unauthenticated attacker to remotely expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives).	2024-01-16	8.8	High
CVE-2024-21673	atlassian - multiple products	This High severity Remote Code Execution (RCE) vulnerability was introduced in versions 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.0 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H allows an authenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release	2024-01-16	8.8	High

		See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives).			
CVE-2024-0517	google - chrome	Out of bounds write in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-16	8.8	High
CVE-2024-0518	google - chrome	Type confusion in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-16	8.8	High
CVE-2024-0519	google - chrome	Out of bounds memory access in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-16	8.8	High
CVE-2023-6548	citrix - multiple products	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gateway allows an attacker with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote code execution on Management Interface.	2024-01-17	8.8	High
CVE-2023-40683	ibm - multiple products	IBM OpenPages with Watson 8.3 and 9.0 could allow remote attacker to bypass security restrictions, caused by insufficient authorization checks. By authenticating as an OpenPages user and using non-public APIs, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrative access to the application. IBM X-Force ID: 264005.	2024-01-19	8.8	High
CVE-2023-47718	ibm - multiple products	IBM Maximo Asset Management 7.6.1.3 and Manage Component 8.10 through 8.11 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 271843.	2024-01-19	8.8	High
CVE-2023-34063	vmware - multiple products	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows.	2024-01-16	8.3	High
CVE-2024-20916	oracle - enterprise_manager	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Event Management). The supported version that is affected is 13.5.0.0. Easily exploitable vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Enterprise Manager Base Platform executes to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, 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 Oracle Enterprise Manager Base Platform accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Manager Base Platform accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L).	2024-01-16	8.3	High
CVE-2023-38738	ibm - multiple products	IBM OpenPages with Watson 8.3 and 9.0 could provide weaker than expected security in a OpenPages environment using Native authentication. If OpenPages is using Native authentication an attacker with access to the OpenPages database could through a series of specially crafted steps could exploit this weakness and gain unauthorized access to other OpenPages accounts. IBM X-Force ID: 262594.	2024-01-19	8.1	High
CVE-2024-0562	linux - multiple products	A use-after-free flaw was found in the Linux Kernel. When a disk is removed, bdi_unregister is called to stop further write-back and waits for associated delayed work to complete. However, wb_inode_writeback_end() may schedule bandwidth estimation work after this has completed, which can result in the timer attempting to access the recently freed bdi_writeback.	2024-01-15	7.8	High
CVE-2024-22428	dell - emc_idrac_service_module	Dell iDRAC Service Module, versions 5.2.0.0 and prior, contain an Incorrect Default Permissions vulnerability. It may allow a local unprivileged user to escalate privileges and execute arbitrary code on the affected system. Dell recommends customers upgrade at the earliest opportunity.	2024-01-16	7.8	High

CVE-2024-0582	linux - multiple products	A memory leak flaw was found in the Linux kernel's io_uring functionality in how a user registers a buffer ring with IORING_REGISTER_PBUF_RING, mmap() it, and then frees it. This flaw allows a local user to crash or potentially escalate their privileges on the system.	2024-01-16	7.8	High
CVE-2024-0646	linux - multiple products	An out-of-bounds memory write flaw was found in the Linux kernel's Transport Layer Security functionality in how a user calls a function splice with a ktls socket as the destination. This flaw allows a local user to crash or potentially escalate their privileges on the system.	2024-01-17	7.8	High
CVE-2021-33631	huawei - multiple products	Integer Overflow or Wraparound vulnerability in openEuler kernel on Linux (filesystem modules) allows Forced Integer Overflow.This issue affects openEuler kernel: from 4.19.90 before 4.19.90-2401.3, from 5.10.0-60.18.0 before 5.10.0-183.0.0.	2024-01-18	7.8	High
CVE-2023-5080	lenovo - tab_m8_hd_tb8505f_firmware	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands.	2024-01-19	7.8	High
CVE-2023-6043	lenovo - vantage	A privilege escalation vulnerability was reported in Lenovo Vantage that could allow a local attacker to bypass integrity checks and execute arbitrary code with elevated privileges.	2024-01-19	7.8	High
CVE-2024-20924	oracle - audit_vault_and_database_firewall	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Audit Vault and Database Firewall, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Audit Vault and Database Firewall. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H).	2024-01-16	7.6	High
CVE-2023-6915	linux - multiple products	A Null pointer dereference problem was found in ida_free in lib/idr.c in the Linux Kernel. This issue may allow an attacker using this library to cause a denial of service problem due to a missing check at a function return.	2024-01-15	7.5	High
CVE-2024-22362	drupal - drupal	Drupal contains a vulnerability with improper handling of structural elements. If this vulnerability is exploited, an attacker may be able to cause a denial-of-service (DoS) condition.	2024-01-16	7.5	High
CVE-2024-21674	atlassian - multiple products	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.6 and a CVSS Vector of CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N allows an unauthenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, no impact to integrity, no impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives).	2024-01-16	7.5	High
CVE-2023-44112	huawei - multiple products	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality.	2024-01-16	7.5	High
CVE-2023-44117	huawei - multiple products	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	High
CVE-2023-4566	huawei - multiple products	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	High

CVE-2023-52109	huawei - multiple products	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	High
CVE-2023-52110	huawei - harmonyos	The sensor module has an out-of-bounds access vulnerability.Successful exploitation of this vulnerability may affect availability.	2024-01-16	7.5	High
CVE-2023-52111	huawei - multiple products	Authorization vulnerability in the BootLoader module. Successful exploitation of this vulnerability may affect service integrity.	2024-01-16	7.5	High
CVE-2023-52113	huawei - multiple products	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability.	2024-01-16	7.5	High
CVE-2023-52098	huawei - multiple products	Denial of Service (DoS) vulnerability in the DMS module. Successful exploitation of this vulnerability will affect availability.	2024-01-16	7.5	High
CVE-2023-52107	huawei - multiple products	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	High
CVE-2023-52108	huawei - multiple products	Vulnerability of process priorities being raised in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability.	2024-01-16	7.5	High
CVE-2023-52114	huawei - multiple products	Data confidentiality vulnerability in the ScreenReader module. Successful exploitation of this vulnerability may affect service integrity.	2024-01-16	7.5	High
CVE-2023-52115	huawei - harmonyos	The iaware module has a Use-After-Free (UAF) vulnerability. Successful exploitation of this vulnerability may affect the system functions.	2024-01-16	7.5	High
CVE-2023-52116	huawei - multiple products	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device.	2024-01-16	7.5	High
CVE-2023-52099	huawei - multiple products	Vulnerability of foreground service restrictions being bypassed in the NMS module. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	High
CVE-2023-52100	huawei - harmonyos	The Celia Keyboard module has a vulnerability in access control. Successful exploitation of this vulnerability may affect availability.	2024-01-16	7.5	High
CVE-2023-52102	huawei - multiple products	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	High
CVE-2023-52104	huawei - multiple products	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	High
CVE-2023-52105	huawei - harmonyos	The nearby module has a privilege escalation vulnerability. Successful exploitation of this vulnerability may affect availability.	2024-01-16	7.5	High
CVE-2024-0553	gnu - gnutls	A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. CVE-2024-0553 is designated as an incomplete resolution for CVE-2023-5981.	2024-01-16	7.5	High
CVE-2024-0567	gnu - gnutls	A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTLS) rejects a certificate chain with distributed trust. This issue occurs when validating a certificate chain with cockpit-certificate-ensure. This flaw allows an unauthenticated, remote client or attacker to initiate a denial of service attack.	2024-01-16	7.5	High
CVE-2024-20932	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 17.0.9; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 21.3.8 and 22.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	2024-01-16	7.5	High
CVE-2023-6549	citrix - multiple products	Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service	2024-01-17	7.5	High
CVE-2023-21901	oracle - multiple products	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that	2024-01-16	7.4	High

		are affected are 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1 and 8.1.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, 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 Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L).			
CVE-2024-20918	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition 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 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2024-01-16	7.4	High
CVE-2024-20952	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2024-01-16	7.4	High
CVE-2023-20258	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. This vulnerability is due to improper processing of serialized Java objects by the affected application. An attacker could exploit this vulnerability by uploading a document containing malicious serialized Java objects to be processed by the affected application. A successful exploit could allow the attacker to cause the application to execute arbitrary commands.	2024-01-17	7.2	High
CVE-2024-20287	cisco - wap371_firmware	A vulnerability in the web-based management interface of the Cisco WAP371 Wireless-AC/N Dual Radio Access Point (AP) with Single Point Setup could allow an authenticated, remote attacker to perform command injection attacks against an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of	2024-01-17	7.2	High

		an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit this vulnerability, the attacker must have valid administrative credentials for the device.			
CVE-2023-6184	citrix - multiple products	Cross SiteScripting vulnerability in Citrix Session Recording allows attacker to perform Cross Site Scripting	2024-01-18	7.2	High
CVE-2023-4001	gnu - grub2	An authentication bypass flaw was found in GRUB due to the way that GRUB uses the UUID of a device to search for the configuration file that contains the password hash for the GRUB password protection feature. An attacker capable of attaching an external drive such as a USB stick containing a file system with a duplicate UUID (the same as in the "/boot/" file system) can bypass the GRUB password protection feature on UEFI systems, which enumerate removable drives before non-removable ones. This issue was introduced in a downstream patch in Red Hat's version of grub2 and does not affect the upstream package.	2024-01-15	6.8	Medium
CVE-2023-6044	lenovo - vantage	A privilege escalation vulnerability was reported in Lenovo Vantage that could allow a local attacker with physical access to impersonate Lenovo Vantage Service and execute arbitrary code with elevated privileges.	2024-01-19	6.8	Medium
CVE-2023-20260	cisco - multiple products	A vulnerability in the application CLI of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager could allow an authenticated, local attacker to gain escalated privileges. This vulnerability is due to improper processing of command line arguments to application scripts. An attacker could exploit this vulnerability by issuing a command on the CLI with malicious options. A successful exploit could allow the attacker to gain the escalated privileges of the root user on the underlying operating system.	2024-01-17	6.7	Medium
CVE-2024-0607	linux - multiple products	A flaw was found in the Netfilter subsystem in the Linux kernel. The issue is in the nft_byteorder_eval() function, where the code iterates through a loop and writes to the `dst` array. On each iteration, 8 bytes are written, but `dst` is an array of u32, so each element only has space for 4 bytes. That means every iteration overwrites part of the previous element corrupting this array of u32. This flaw allows a local user to cause a denial of service or potentially break NetFilter functionality.	2024-01-18	6.6	Medium
CVE-2023-46749	apache - multiple products	Apache Shiro before 1.13.0 or 2.0.0-alpha-4, may be susceptible to a path traversal attack that results in an authentication bypass when used together with path rewriting Mitigation: Update to Apache Shiro 1.13.0+ or 2.0.0-alpha-4+, or ensure `blockSemicolon` is enabled (this is the default).	2024-01-15	6.5	Medium
CVE-2023-50290	apache - solr	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Solr. The Solr Metrics API publishes all unprotected environment variables available to each Apache Solr instance. Users are able to specify which environment variables to hide, however, the default list is designed to work for known secret Java system properties. Environment variables cannot be strictly defined in Solr, like Java system properties can be, and may be set for the entire host, unlike Java system properties which are set per-Java-proccess. The Solr Metrics API is protected by the "metrics-read" permission. Therefore, Solr Clouds with Authorization setup will only be vulnerable via users with the "metrics-read" permission. This issue affects Apache Solr: from 9.0.0 before 9.3.0. Users are recommended to upgrade to version 9.3.0 or later, in which environment variables are not published via the Metrics API.	2024-01-15	6.5	Medium
CVE-2024-20961	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 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).	2024-01-16	6.5	Medium
CVE-2024-20963	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.35 and prior and 8.2.0 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	2024-01-16	6.5	Medium

		(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).			
CVE-2024-20973	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 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).	2024-01-16	6.5	Medium
CVE-2024-20975	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.2.0 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).	2024-01-16	6.5	Medium
CVE-2024-20977	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 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).	2024-01-16	6.5	Medium
CVE-2024-20985	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.35 and prior and 8.2.0 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).	2024-01-16	6.5	Medium
CVE-2023-20271	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database.	2024-01-17	6.5	Medium
CVE-2024-20930	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).	2024-01-16	6.3	Medium
CVE-2024-20908	oracle - webcenter_sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: Advanced UI). 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 Sites. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data as well as unauthorized read access to a subset of Oracle WebCenter Sites 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).	2024-01-16	6.1	Medium
CVE-2024-20928	oracle - webcenter_content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported	2024-01-16	6.1	Medium

		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 require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data as well as unauthorized read access to a subset of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 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-2024-20934	oracle - installed_base	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: Engineering Change Order). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Installed Base, 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 Installed Base accessible data as well as unauthorized read access to a subset of Oracle Installed Base 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).	2024-01-16	6.1	Medium
CVE-2024-20936	oracle - one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Documents). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, 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 One-to-One Fulfillment accessible data as well as unauthorized read access to a subset of Oracle One-to-One Fulfillment 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).	2024-01-16	6.1	Medium
CVE-2024-20938	oracle - istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: ECC). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, 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 iStore accessible data as well as unauthorized read access to a subset of Oracle iStore 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).	2024-01-16	6.1	Medium
CVE-2024-20940	oracle - knowledge_management	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Create, Update, Authoring Flow). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data as well as unauthorized read access to a subset of Oracle Knowledge Management 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).	2024-01-16	6.1	Medium
CVE-2024-20942	oracle - multiple products	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: LOV). Supported versions that are affected are 11.5, 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in	2024-01-16	6.1	Medium

		unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul 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-2024-20948	oracle - knowledge_management	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Setup, Admin). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data as well as unauthorized read access to a subset of Oracle Knowledge Management 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).	2024-01-16	6.1	Medium
CVE-2024-20950	oracle - customer_interaction_history	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, 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 Customer Interaction History accessible data as well as unauthorized read access to a subset of Oracle Customer Interaction History 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).	2024-01-16	6.1	Medium
CVE-2024-20926	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition 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 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2024-01-16	5.9	Medium
CVE-2024-20709	adobe - multiple products	Acrobat Reader T5 (MSFT Edge) versions 120.0.2210.91 and earlier are affected by an Improper Input Validation vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-01-15	5.5	Medium
CVE-2024-20721	adobe - multiple products	Acrobat Reader T5 (MSFT Edge) versions 120.0.2210.91 and earlier are affected by an Improper Input Validation vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-01-15	5.5	Medium
CVE-2024-0584	linux - multiple products	A use-after-free issue was found in igmp_start_timer in net/ipv4/igmp.c in the network sub-component in the Linux Kernel. This flaw allows a local user to observe a refcnt use-after-free issue when receiving an igmp query packet, leading to a kernel information leak.	2024-01-16	5.5	Medium
CVE-2024-20946	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. CVSS 3.1 Base	2024-01-16	5.5	Medium

		Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).			
CVE-2024-20967	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	2024-01-16	5.5	Medium
CVE-2024-20969	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	2024-01-16	5.5	Medium
CVE-2024-0639	linux - linux_kernel	A denial of service vulnerability due to a deadlock was found in sctp_auto_asconf_init in net/sctp/socket.c in the Linux kernel's SCTP subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system.	2024-01-17	5.5	Medium
CVE-2024-0641	linux - multiple products	A denial of service vulnerability was found in tipc_crypto_key_revoke in net/tipc/crypto.c in the Linux kernel's TIPC subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system.	2024-01-17	5.5	Medium
CVE-2023-48340	google - multiple products	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48341	google - multiple products	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48343	google - multiple products	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48344	google - multiple products	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48345	google - multiple products	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48346	google - multiple products	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48347	google - multiple products	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48348	google - multiple products	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48349	google - multiple products	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48350	google - multiple products	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48351	google - multiple products	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48352	google - multiple products	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2023-48354	google - multiple products	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed	2024-01-18	5.5	Medium
CVE-2021-33630	huawei - openeuler	NULL Pointer Dereference vulnerability in openEuler kernel on Linux (network modules) allows Pointer Manipulation. This vulnerability is associated with program files net/sched/sch_cbs.C. This issue affects openEuler kernel: from 4.19.90 before 4.19.90-2401.3.	2024-01-18	5.5	Medium

CVE-2023-6450	lenovo - app_store	An incorrect permissions vulnerability was reported in the Lenovo App Store app that could allow an attacker to use system resources, resulting in a denial of service.	2024-01-19	5.5	Medium
CVE-2024-20944	oracle - isupport	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, 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 iSupport accessible data as well as unauthorized read access to a subset of Oracle iSupport 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).	2024-01-16	5.4	Medium
CVE-2024-20979	oracle - multiple products	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0, 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 BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle 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 Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle 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).	2024-01-16	5.4	Medium
CVE-2024-20987	oracle - bi_publisher	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle 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 Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle 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).	2024-01-16	5.4	Medium
CVE-2024-20251	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-01-17	5.4	Medium
CVE-2024-20270	cisco - multiple products	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-01-17	5.4	Medium
CVE-2023-51463	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-01-18	5.4	Medium
CVE-2023-51464	adobe - multiple products	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-01-18	5.4	Medium

CVE-2023-49943	zohocorp - multiple products	Zoho ManageEngine ServiceDesk Plus MSP before 14504 allows stored XSS (by a low-privileged technician) via a task's name in a time sheet.	2024-01-18	5.4	Medium
CVE-2023-32337	ibm - multiple products	IBM Maximo Spatial Asset Management 8.10 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: 255288.	2024-01-19	5.4	Medium
CVE-2023-50963	ibm - storage_defender_data_protect	IBM Storage Defender - Data Protect 1.0.0 through 1.4.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 276101.	2024-01-19	5.4	Medium
CVE-2023-52112	huawei - multiple products	Unauthorized file access vulnerability in the wallpaper service module. Successful exploitation of this vulnerability may cause features to perform abnormally.	2024-01-16	5.3	Medium
CVE-2023-50950	ibm - multiple products	IBM QRadar SIEM 7.5 could disclose sensitive email information in responses from offense rules. IBM X-Force ID: 275709.	2024-01-17	5.3	Medium
CVE-2023-35020	ibm - sterling_control_center	IBM Sterling Control Center 6.3.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257874.	2024-01-19	5.3	Medium
CVE-2024-21733	apache - multiple products	Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.	2024-01-19	5.3	Medium
CVE-2024-20904	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 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. 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 read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2024-01-16	5	Medium
CVE-2024-20965	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 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).	2024-01-16	4.9	Medium
CVE-2024-20971	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 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).	2024-01-16	4.9	Medium
CVE-2024-20981	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 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).	2024-01-16	4.9	Medium
CVE-2024-20983	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). 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).	2024-01-16	4.9	Medium

CVE-2024-20906	oracle - multiple products	Vulnerability in the Integrated Lights Out Manager (ILOM) product of Oracle Systems (component: System Management). Supported versions that are affected are 3, 4 and 5. Easily exploitable vulnerability allows high privileged attacker with network access via ICMP to compromise Integrated Lights Out Manager (ILOM). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Integrated Lights Out Manager (ILOM), 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 Integrated Lights Out Manager (ILOM) accessible data as well as unauthorized read access to a subset of Integrated Lights Out Manager (ILOM) accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	4.8	Medium
CVE-2023-20257	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct cross-site scripting attacks. This vulnerability is due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by submitting malicious input containing script or HTML content within requests that would stored within the application interface. A successful exploit could allow the attacker to conduct cross-site scripting attacks against other users of the affected application.	2024-01-17	4.8	Medium
CVE-2023-49515	tp-link - multiple products	Insecure Permissiosn vulnerability in TP Link TC70 and C200 WIFI Camera v.3 firmware v.1.3.4 and fixed in v.1.3.11 allows a physically proximate attacker to obtain sensitive information via a connection to the UART pin components.	2024-01-17	4.6	Medium
CVE-2024-20959	oracle - zfs_storage_appliance_kit	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	4.4	Medium
CVE-2023-48339	google - multiple products	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	2024-01-18	4.4	Medium
CVE-2023-48342	google - multiple products	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2024-01-18	4.4	Medium
CVE-2023-48353	google - multiple products	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed	2024-01-18	4.4	Medium
CVE-2023-48355	google - multiple products	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2024-01-18	4.4	Medium
CVE-2023-48356	google - multiple products	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2024-01-18	4.4	Medium
CVE-2023-48357	google - multiple products	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2024-01-18	4.4	Medium
CVE-2023-48358	google - multiple products	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2024-01-18	4.4	Medium
CVE-2023-48359	google - multiple products	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed	2024-01-18	4.4	Medium
CVE-2024-20920	oracle - solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2024-01-16	3.8	Low
CVE-2024-20955	oracle - multiple products	Vulnerability in the Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple	2024-01-16	3.7	Low

		protocols to compromise Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition 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).			
CVE-2023-5081	lenovo - tab_m8_hd_tb8505f_firmware	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier.	2024-01-19	3.3	Low
CVE-2024-20910	oracle - audit_vault_and_database_firewall	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. While the vulnerability is in Oracle Audit Vault and Database Firewall, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Audit Vault and Database Firewall accessible data. CVSS 3.1 Base Score 3.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N).	2024-01-16	3	Low
CVE-2024-20912	oracle - audit_vault_and_database_firewall	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Easily exploitable vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Audit Vault and Database Firewall accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2024-01-16	2.7	Low
CVE-2024-20957	oracle - jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Package Build SEC). Supported versions that are affected are Prior to 9.2.8.1. Easily exploitable vulnerability allows high privileged attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2024-01-16	2.7	Low
CVE-2024-20922	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u391; Oracle GraalVM Enterprise Edition: 20.3.12 and 21.3.8. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM 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 Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	2024-01-16	2.5	Low
CVE-2024-20914	oracle - zfs_storage_appliance_kit	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 2.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2024-01-16	2.3	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.