الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
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.

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 18th of January to 24th 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

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

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 18 يناير إلى 24 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 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
CVE-2026-21962	oracle - multiple products	Vulnerability in the Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in product of Oracle Fusion Middleware (component: Weblogic Server Proxy Plug-in for Apache HTTP Server, Weblogic Server Proxy Plug-in for IIS). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in. While the vulnerability is in Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in, 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 HTTP Server, Oracle Weblogic Server Proxy Plug-in accessible data as well as unauthorized access to critical data or complete access to all Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in accessible data. Note: Affected version for Weblogic Server Proxy Plug-in for IIS is 12.2.1.4.0 only. CVSS 3.1 Base Score 10.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-01-20	10
CVE-2026-24304	microsoft - Azure Resource Manager	Improper access control in Azure Resource Manager allows an authorized attacker to elevate privileges over a network.	2026-01-23	9.9
CVE-2026-0905	google - chrome	Insufficient policy enforcement in Network in Google Chrome prior to 144.0.7559.59 allowed an attack who obtained a network log file to potentially obtain potentially sensitive information via a network log file. (Chromium security severity: Medium)	2026-01-20	9.8
CVE-2026-0906	google - chrome	Incorrect security UI in Google Chrome on Android prior to 144.0.7559.59 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low)	2026-01-20	9.8
CVE-2026-0907	google - chrome	Incorrect security UI in Split View in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-01-20	9.8
CVE-2026-21969	oracle - agile_product_lifecycle_management_for_process	Vulnerability in the Oracle Agile Product Lifecycle Management for Process product of Oracle Supply Chain (component: Supplier Portal). The supported version that is affected is 6.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile Product Lifecycle Management for Process. Successful attacks of this vulnerability can result in takeover of Oracle Agile Product Lifecycle Management for Process. 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).	2026-01-20	9.8
CVE-2026-24061	gnu - inetutils	telnetd in GNU Inetutils through 2.7 allows remote authentication bypass via a "-f root" value for the USER environment variable.	2026-01-21	9.8
CVE-2026-24306	microsoft - Azure Front Door	Improper access control in Azure Front Door (AFD) allows an unauthorized attacker to elevate privileges over a network.	2026-01-22	9.8
CVE-2026-21264	microsoft - Microsoft Account	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Account allows an unauthorized attacker to perform spoofing over a network.	2026-01-22	9.3
CVE-2026-24305	microsoft - Microsoft Entra	Azure Entra ID Elevation of Privilege Vulnerability	2026-01-22	9.3
CVE-2026-24307	microsoft - Microsoft 365 Copilot	Improper validation of specified type of input in M365 Copilot allows an unauthorized attacker to disclose information over a network.	2026-01-22	9.3
CVE-2026-0899	google - chrome	Out of bounds memory access in V8 in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	2026-01-20	8.8

CVE-2026-0900	google - chrome	Inappropriate implementation in V8 in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	2026-01-20	8.8
CVE-2026-0902	google - chrome	Inappropriate implementation in V8 in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2026-01-20	8.8
CVE-2026-0908	google - chrome	Use after free in ANGLE in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)	2026-01-20	8.8
CVE-2025-33015	ibm - concert	IBM Concert 1.0.0 through 2.1.0 is vulnerable to malicious file upload by not validating the content of the file uploaded to the web interface.	2026-01-20	8.8
CVE-2025-36588	dell - multiple products	Dell Unisphere for PowerMax, version(s) 10.2.0.x, contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	2026-01-22	8.8
CVE-2026-22273	dell - ObjectScale	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0, contains an Use of Default Credentials vulnerability in the OS. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-01-23	8.8
CVE-2026-21967	oracle - multiple products	Vulnerability in the Oracle Hospitality OPERA 5 product of Oracle Hospitality Applications (component: Opera Servlet). Supported versions that are affected are 5.6.19.23, 5.6.25.17, 5.6.26.10 and 5.6.27.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality OPERA 5 accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality OPERA 5. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L).	2026-01-20	8.6
CVE-2026-1260	google - sentencepiece	Invalid memory access in Sentencepiece versions less than 0.2.1 when using a vulnerable model file, which is not created in the normal training procedure.	2026-01-22	8.5
CVE-2025-12985	ibm - IBM Licensing Operator	IBM Licensing Operator incorrectly assigns privileges to security critical files which could allow a local root escalation inside a container running the IBM Licensing Operator image.	2026-01-20	8.4
CVE-2025-14115	ibm - Sterling Connect:Direct for UNIX Container	IBM Sterling Connect:Direct for UNIX Container 6.3.0.0 through 6.3.0.6 Interim Fix 016, and 6.4.0.0 through 6.4.0.3 Interim Fix 019 IBM® Sterling Connect:Direct for UNIX 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.	2026-01-20	8.4
CVE-2026-21955	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-01-20	8.2
CVE-2026-21956	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-01-20	8.2
CVE-2026-21987	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-01-20	8.2
CVE-2026-21988	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-01-20	8.2
CVE-2026-21990	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-01-20	8.2
CVE-2026-22022	apache - solr	Deployments of Apache Solr 5.3.0 through 9.10.0 that rely on Solr's "Rule Based Authorization Plugin" are vulnerable to allowing unauthorized access to certain Solr APIs, due to insufficiently strict input validation in those components. Only deployments that meet all of the following criteria are impacted by this vulnerability: * Use of Solr's "RuleBasedAuthorizationPlugin" * A RuleBasedAuthorizationPlugin config (see security.json) that specifies multiple "roles" * A RuleBasedAuthorizationPlugin permission list (see security.json) that uses one or more of the following pre-defined permission rules: "config-read", "config-edit", "schema-read", "metrics-read", or "security-read".	2026-01-21	8.2

		* A RuleBasedAuthorizationPlugin permission list that doesn't define the "all" pre-defined permission * A networking setup that allows clients to make unfiltered network requests to Solr. (i.e. user-submitted HTTP/HTTPS requests reach Solr as-is, unmodified or restricted by any intervening proxy or gateway) Users can mitigate this vulnerability by ensuring that their RuleBasedAuthorizationPlugin configuration specifies the "all" pre-defined permission and associates the permission with an "admin" or other privileged role. Users can also upgrade to a Solr version outside of the impacted range, such as the recently released Solr 9.10.1.		
CVE-2026-20045	cisco - multiple products	A vulnerability in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P), Cisco Unity Connection, and Cisco Webex Calling Dedicated Instance could allow an unauthenticated, remote attacker&nbsp;to execute arbitrary commands on the underlying operating system of an affected device.&nbsp;_x000D_ _x000D_ This vulnerability is due to improper validation of user-supplied input in HTTP requests. An attacker could exploit this vulnerability by sending a sequence of crafted HTTP requests to the web-based management interface of an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root._x000D_ Note: Cisco has assigned this security advisory a Security Impact Rating (SIR) of Critical rather than High as the score indicates. The reason is that exploitation of this vulnerability could result in an attacker elevating privileges to root.	2026-01-21	8.2
CVE-2026-21227	microsoft - Azure Logic Apps	Improper limitation of a pathname to a restricted directory ('path traversal') in Azure Logic Apps allows an unauthorized attacker to elevate privileges over a network.	2026-01-22	8.2
CVE-2026-21989	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. 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 creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L).	2026-01-20	8.1
CVE-2026-22278	dell - powerscale_onefs	Dell PowerScale OneFS versions prior to 9.13.0.0 contains an improper restriction of excessive authentication attempts vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-01-22	8.1
CVE-2026-20613	apple - multiple products	The ArchiveReader.extractContents() function used by cctl image load and container image load performs no pathname validation before extracting an archive member. This means that a carelessly or maliciously constructed archive can extract a file into any user-writable location on the system using relative pathnames. This issue is addressed in container 0.8.0 and containerization 0.21.0.	2026-01-23	7.8
CVE-2025-29847	apache - linkis	A vulnerability in Apache Linkis. Problem Description When using the JDBC engine and da When using the JDBC engine and data source functionality, if the URL parameter configured on the frontend has undergone multiple rounds of URL encoding, it may bypass the system's checks. This bypass can trigger a vulnerability that allows unauthorized access to system files via JDBC parameters. Scope of Impact This issue affects Apache Linkis: from 1.3.0 through 1.7.0. Severity level moderate Solution Continuously check if the connection information contains the "%" character; if it does, perform URL decoding. Users are recommended to upgrade to version 1.8.0, which fixes the issue. More questions about this vulnerability can be discussed here: https://lists.apache.org/list?dev@linkis.apache.org:2025-9:cve	2026-01-19	7.5
CVE-2026-21926	oracle - siebel_customer_relationship_management_deployment	Vulnerability in the Siebel CRM Deployment product of Oracle Siebel CRM (component: Server Infrastructure). Supported versions that are affected are 17.0-25.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Siebel CRM Deployment. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Siebel CRM Deployment. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-01-20	7.5

CVE-2026-21940	oracle - supply_chain_products_suite	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: User and User Group). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM 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).	2026-01-20	7.5
CVE-2026-21945	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: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. 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 ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability 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 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-01-20	7.5
CVE-2026-21957	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-01-20	7.5
CVE-2026-21982	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-01-20	7.5
CVE-2026-21983	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-01-20	7.5
CVE-2026-21984	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-01-20	7.5
CVE-2026-21520	microsoft - Microsoft Copilot Studio	Exposure of Sensitive Information to an Unauthorized Actor in Copilot Studio allows a unauthenticated attacker to view sensitive information through network attack vector	2026-01-22	7.5
CVE-2026-22271	dell - ObjectScale	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0, contains a Cleartext Transmission of Sensitive Information vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information exposure.	2026-01-23	7.5
CVE-2026-21932	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: AWT, JavaFX). Supported versions that are affected are Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. 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 require human interaction from a person other than the attacker and while the vulnerability is in Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, 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 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 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N).	2026-01-20	7.4
CVE-2026-21521	microsoft - Microsoft 365 Word Copilot	Improper neutralization of escape, meta, or control sequences in Copilot allows an unauthorized attacker to disclose information over a network.	2026-01-22	7.4
CVE-2026-21524	microsoft - Azure Data Explorer	Exposure of sensitive information to an unauthorized actor in Azure Data Explorer allows an unauthorized attacker to disclose information over a network.	2026-01-22	7.4
CVE-2025-36418	ibm - applinx	IBM ApplinX 11.1 is vulnerable due to a privilege escalation vulnerability due to improper verification of JWT tokens. An attacker may be able to craft or modify a JSON web token in order to impersonate another user or to elevate their privileges.	2026-01-20	7.3

CVE-2026-21976	oracle - multiple products	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Oracle Analytics Cloud). Supported versions that are affected are 7.6.0.0.0 and 8.2.0.0.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Business Intelligence Enterprise Edition executes to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-01-20	7.1
CVE-2026-21986	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows unauthenticated 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. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 7.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H).	2026-01-20	7.1
CVE-2026-22444	apache - solr	The "create core" API of Apache Solr 8.6 through 9.10.0 lacks sufficient input validation on some API parameters, which can cause Solr to check the existence of and attempt to read file-system paths that should be disallowed by Solr's "allowPaths" security setting https://https://solr.apache.org/guide/solr/latest/configuration-guide/configuring-solr-xml.html#the-solr-element . These read-only accesses can allow users to create cores using unexpected configsets if any are accessible via the filesystem. On Windows systems configured to allow UNC paths this can additionally cause disclosure of NTLM "user" hashes. Solr deployments are subject to this vulnerability if they meet the following criteria: * Solr is running in its "standalone" mode. * Solr's "allowPath" setting is being used to restrict file access to certain directories. * Solr's "create core" API is exposed and accessible to untrusted users. This can happen if Solr's RuleBasedAuthorizationPlugin https://solr.apache.org/guide/solr/latest/deployment-guide/rule-based-authorization-plugin.html is disabled, or if it is enabled but the "core-admin-edit" predefined permission (or an equivalent custom permission) is given to low-trust (i.e. non-admin) user roles. Users can mitigate this by enabling Solr's RuleBasedAuthorizationPlugin (if disabled) and configuring a permission-list that prevents untrusted users from creating new Solr cores. Users should also upgrade to Apache Solr 9.10.1 or greater, which contain fixes for this issue.	2026-01-21	7.1
CVE-2026-21939	oracle - database_server	Vulnerability in the SQLcl component of Oracle Database Server. Supported versions that are affected are 23.4.0-23.26.0. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where SQLcl executes to compromise SQLcl. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of SQLcl. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-01-20	7

CVE-2025-59355	apache - linkis	A vulnerability.
		When org.apache.linkis.metadata.util.HiveUtils.decode() fails to perform Base64 decoding, it records the complete input parameter string in the log via logger.error(str + "decode failed", e). If the input parameter contains sensitive information such as Hive Metastore keys, plaintext passwords will be left in the log files when decoding fails, resulting in information leakage.
		Affected Scope
		Component: Sensitive fields in hive-site.xml (e.g., javax.jdo.option.ConnectionPassword) or other fields encoded in Base64.
		Version: Apache Linkis 1.0.0 – 1.7.0
		Trigger Conditions
		The value of the configuration item is an invalid Base64 string.
		Log files are readable by users other than hive-site.xml administrators.
		Severity: Low
		The probability of Base64 decoding failure is low.
		The leakage is only triggered when logs at the Error level are exposed.
		Remediation
		Apache Linkis 1.8.0 and later versions have replaced the log with desensitized content.
		logger.error("URL decode failed: {}", e.getMessage()); // 不再输出 str
		Users are recommended to upgrade to version 1.8.0, which fixes the issue.
			2026-01-19	6.5

CVE-2026-21923	oracle - life_sciences_central_designer	Vulnerability in the Oracle Life Sciences Central Designer product of Oracle Health Sciences Applications (component: Platform). The supported version that is affected is 7.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Life Sciences Central Designer. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Life Sciences Central Designer accessible data as well as unauthorized read access to a subset of Oracle Life Sciences Central	2026-01-20	6.5

		Designer 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).		
CVE-2026-21944	oracle - agile_product_lifecycle_management_for_process	Vulnerability in the Oracle Agile Product Lifecycle Management for Process product of Oracle Supply Chain (component: Product Quality Management). The supported version that is affected is 6.2.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile Product Lifecycle Management for Process. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile Product Lifecycle Management for Process 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).	2026-01-20	6.5
CVE-2026-21949	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.5.0. 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).	2026-01-20	6.5
CVE-2026-21950	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.5.0. 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).	2026-01-20	6.5
CVE-2026-21960	oracle - applications_dba	Vulnerability in the Oracle Applications DBA product of Oracle E-Business Suite (component: Java utils). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications DBA. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications DBA accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications DBA accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	2026-01-20	6.5
CVE-2026-21968	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. 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).	2026-01-20	6.5
CVE-2026-21970	oracle - life_sciences_central_designer	Vulnerability in the Oracle Life Sciences Central Designer product of Oracle Health Sciences Applications (component: Platform). The supported version that is affected is 7.0.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Life Sciences Central Designer. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Life Sciences Central Designer 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).	2026-01-20	6.5
CVE-2026-21980	oracle - life_sciences_central_coding	Vulnerability in the Oracle Life Sciences Central Coding product of Oracle Health Sciences Applications (component: Platform). The supported version that is affected is 7.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Life Sciences Central Coding. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Life Sciences Central Coding accessible data as well as unauthorized read access to a subset of Oracle Life Sciences Central Coding 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).	2026-01-20	6.5
CVE-2025-14559	red hat - Red Hat Build of Keycloak	A flaw was found in the keycloak-services component of Keycloak. This vulnerability allows the issuance of access and refresh tokens for disabled users, leading to unauthorized use of previously revoked privileges, via a business logic vulnerability in the Token Exchange implementation when a privileged client invokes the token exchange flow.	2026-01-21	6.5
CVE-2026-22274	dell - ObjectScale	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0, contains a Cleartext Transmission of Sensitive Information vulnerability in the Fabric Syslog. An unauthenticated attacker with remote access could potentially exploit this vulnerability to intercept and modify information in transit.	2026-01-23	6.5
CVE-2025-36408	ibm - applinx	IBM ApplinX 11.1 is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-01-20	6.4
CVE-2025-36063	ibm - Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0	IBM Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0 5.2.0.00 through 5.2.0.12 does not invalidate session after a logout which could allow an authenticated user to impersonate another user on the system.	2026-01-20	6.3
CVE-2025-36065	ibm - Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0	IBM Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0 5.2.0.00 through 5.2.0.12 does not invalidate session after a browser closure which could allow an authenticated user to impersonate another user on the system.	2026-01-20	6.3
CVE-2025-36115	ibm - Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0	IBM Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0.00 through 5.2.0.12 does not disallow the session id after use which could allow an authenticated user to impersonate another user on the system.	2026-01-20	6.3
CVE-2025-36066	ibm - Sterling Connect:Express Adapter for	IBM Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0 5.2.0.00 through 5.2.0.12 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed	2026-01-20	6.1

	Sterling B2B Integrator 5.2.0	arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.		
CVE-2026-21933	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. 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 require human interaction from a person other than the attacker and while the vulnerability is in Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of 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 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).	2026-01-20	6.1
CVE-2026-21938	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.60, 8.61 and 8.62. 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).	2026-01-20	6.1
CVE-2026-21943	oracle - scripting	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Scripting Admin). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Scripting accessible data as well as unauthorized read access to a subset of Oracle Scripting accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-01-20	6.1
CVE-2026-21946	oracle - jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are 9.2.0.0-9.2.26.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-01-20	6.1
CVE-2026-21951	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Integration Broker). Supported versions that are affected are 8.60, 8.61 and 8.62. 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).	2026-01-20	6.1
CVE-2026-21961	oracle - peoplesoft_enterprise_hcm_human_resources	Vulnerability in the PeopleSoft Enterprise HCM Human Resources product of Oracle PeopleSoft (component: Company Dir / Org Chart Viewer, Employee Snapshot). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Human Resources, 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 HCM Human Resources accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources accessible data. CVSS 3.1 Base Score 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).	2026-01-20	6.1
CVE-2026-21966	oracle - multiple products	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). Supported versions that are affected are 5.6.19.23, 5.6.25.17, 5.6.26.10 and 5.6.27.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality OPERA 5 Property Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality OPERA 5 Property Services accessible data as well as unauthorized read access to a subset of Oracle Hospitality OPERA 5 Property Services	2026-01-20	6.1

		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-2026-21963	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2026-01-20	6
CVE-2026-21985	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2026-01-20	6
CVE-2026-20092	cisco - Cisco Intersight Virtual Appliance	A vulnerability in the read-only maintenance shell of Cisco Intersight Virtual Appliance could allow an authenticated, local attacker with administrative privileges to elevate privileges to root on the virtual appliance._x000D_ _x000D_ This vulnerability is due to improper file permissions on configuration files for system accounts within the maintenance shell of the virtual appliance. An attacker could exploit this vulnerability by accessing the maintenance shell as a read-only administrator and manipulating system files to grant root privileges. A successful exploit could allow the attacker to elevate their privileges to&nbsp;root on the virtual appliance and gain full control of the appliance, giving them the ability to access sensitive information, modify workloads and configurations on the host system, and cause a denial of service (DoS).	2026-01-21	6
CVE-2025-1719	ibm - concert	IBM Concert 1.0.0 through 2.1.0 could allow a remote attacker to obtain sensitive information from allocated memory due to improper clearing of heap memory.	2026-01-20	5.9
CVE-2025-1722	ibm - concert	IBM Concert 1.0.0 through 2.1.0 could allow a remote attacker to obtain sensitive information from allocated memory due to improper clearing of heap memory.	2026-01-20	5.9
CVE-2026-1180	red hat - multiple products	A flaw was identified in Keycloak's OpenID Connect Dynamic Client Registration feature when clients authenticate using private_key_jwt. The issue allows a client to specify an arbitrary jwks_uri, which Keycloak then retrieves without validating the destination. This enables attackers to coerce the Keycloak server into making HTTP requests to internal or restricted network resources. As a result, attackers can probe internal services and cloud metadata endpoints, creating an information disclosure and reconnaissance risk.	2026-01-20	5.8
CVE-2026-21927	oracle - multiple products	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Driver). The supported version that is affected is 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Solaris accessible data as well as unauthorized access to critical data or complete access to all Oracle Solaris accessible data. CVSS 3.1 Base Score 5.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N).	2026-01-20	5.8
CVE-2026-21935	oracle - solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Driver). The supported version that is affected is 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Solaris accessible data as well as unauthorized access to critical data or complete access to all Oracle Solaris accessible data. CVSS 3.1 Base Score 5.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N).	2026-01-20	5.8
CVE-2025-36058	ibm - Business Automation Workflow containers	IBM Business Automation Workflow containers 25.0.0 through 25.0.0 Interim Fix 002, 24.0.1 through 24.0.1 Interim Fix 005, and 24.0.0 through 24.0.0 Interim Fix 006. IBM Cloud Pak for Business Automation and IBM Business Automation Workflow containers may disclose sensitve configuration information in a config map.	2026-01-20	5.5
CVE-2026-22276	dell - ObjectScale	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0, contains a Cleartext Storage of Sensitive Information vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2026-01-23	5.5
CVE-2026-0901	google - chrome	Inappropriate implementation in Blink in Google Chrome on Android prior to 144.0.7559.59 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: High)	2026-01-20	5.4
CVE-2026-0903	google - chrome	Inappropriate implementation in Downloads in Google Chrome on Windows prior to 144.0.7559.59 allowed a remote attacker to bypass dangerous file type protections via a malicious file. (Chromium security severity: Medium)	2026-01-20	5.4
CVE-2026-0904	google - chrome	Incorrect security UI in Digital Credentials in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-01-20	5.4
CVE-2025-36113	ibm - Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0	IBM Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0 5.2.0.00 through 5.2.0.12 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-01-20	5.4
CVE-2025-36396	ibm - application_gateway	IBM Application Gateway 23.10 through 25.09 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-01-20	5.4

CVE-2025-36397	ibm - application_gateway	IBM Application Gateway 23.10 through 25.09 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site.	2026-01-20	5.4
CVE-2025-36409	ibm - applinx	IBM ApplinX 11.1 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-01-20	5.4
CVE-2026-21924	oracle - multiple products	Vulnerability in the Oracle Utilities Application Framework product of Oracle Utilities Applications (component: General). Supported versions that are affected are 4.4.0.3.0, 4.5.0.0.0, 4.5.0.1.1, 4.5.0.1.3, 4.5.0.2.0, 25.4 and 25.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Utilities Application Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Utilities Application 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 Utilities Application Framework accessible data as well as unauthorized read access to a subset of Oracle Utilities Application Framework 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).	2026-01-20	5.4
CVE-2026-21931	oracle - multiple products	Vulnerability in the Oracle APEX Sample Applications product of Oracle APEX (component: Brookstrut Sample App). Supported versions that are affected are 23.2.0, 23.2.1, 24.1.0, 24.2.0 and 24.2.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle APEX Sample Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle APEX Sample Applications, 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 APEX Sample Applications accessible data as well as unauthorized read access to a subset of Oracle APEX Sample Applications 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).	2026-01-20	5.4
CVE-2026-21934	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Push Notifications). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. 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 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-01-20	5.4
CVE-2026-21971	oracle - peoplesoft_supply_chain_management_purchasing	Vulnerability in the PeopleSoft Enterprise SCM Purchasing product of Oracle PeopleSoft (component: Purchasing). 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 SCM Purchasing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM Purchasing accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM Purchasing accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-01-20	5.4
CVE-2025-36419	ibm - applinx	IBM ApplinX 11.1 could disclose sensitive information about server architecture that could aid in further attacks against the system.	2026-01-20	5.3
CVE-2026-21928	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 unauthenticated attacker with network access via TCP to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris 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).	2026-01-20	5.3
CVE-2026-21929	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 9.0.0-9.5.0. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	2026-01-20	5.3
CVE-2026-21972	oracle - configurator	Vulnerability in the Oracle Configurator product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Configurator 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).	2026-01-20	5.3
CVE-2026-21974	oracle - life_sciences_central_designer	Vulnerability in the Oracle Life Sciences Central Designer product of Oracle Health Sciences Applications (component: Platform). The supported version that is affected is 7.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Life Sciences Central Designer. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Life Sciences Central Designer 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).	2026-01-20	5.3
CVE-2026-20080	cisco - Cisco Ultra-Reliable Wireless Backhaul	A vulnerability in the SSH service of Cisco IEC6400 Wireless Backhaul Edge Compute Software could allow an unauthenticated, remote attacker to cause the SSH service to stop responding._x000D_ _x000D_ This vulnerability exists because the SSH service lacks effective flood protection. An attacker could exploit this vulnerability by initiating a denial of service (DoS) attack against the SSH port. A successful exploit could allow the attacker to cause the SSH service to be unresponsive during the period of the DoS attack. All other operations remain stable during the attack.	2026-01-21	5.3
CVE-2026-21942	oracle - multiple products	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystems). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle	2026-01-20	5

		Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H).		
CVE-2026-22280	dell - multiple products	Dell PowerScale OneFS, versions 9.5.0.0 through 9.5.1.5, versions 9.6.0.0 through 9.7.1.10, versions 9.8.0.0 through 9.10.1.3, versions starting from 9.11.0.0 and prior to 9.13.0.0, contains an incorrect permission assignment for critical resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service.	2026-01-22	5
CVE-2025-13925	ibm - aspera_console	IBM Aspera Console 3.4.7 stores potentially sensitive information in log files that could be read by a local privileged user.	2026-01-20	4.9
CVE-2026-21936	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. 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).	2026-01-20	4.9
CVE-2026-21937	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. 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).	2026-01-20	4.9
CVE-2026-21941	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. 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).	2026-01-20	4.9
CVE-2026-21948	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. 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).	2026-01-20	4.9
CVE-2026-21952	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 9.0.0-9.5.0. 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).	2026-01-20	4.9
CVE-2026-21959	oracle - workflow	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Loader). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Workflow accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2026-01-20	4.9
CVE-2026-21964	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. 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).	2026-01-20	4.9
CVE-2026-21925	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: RMI). Supported versions that are affected are Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. 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 update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of 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 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).	2026-01-20	4.8
CVE-2026-20055	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Packaged Contact Center Enterprise (Packaged CCE) and Cisco Unified Contact Center Enterprise (Unified CCE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device.&nbsp;_x000D_ _x000D_ These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities 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. To exploit these vulnerabilities, the attacker must have valid administrative credentials.	2026-01-21	4.8
CVE-2026-20109	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Packaged Contact Center Enterprise (Packaged CCE) and Cisco Unified Contact Center Enterprise (Unified CCE) could allow an	2026-01-21	4.8

		authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device.&nbsp;_x000D_ _x000D_ These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities 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. To exploit these vulnerabilities, the attacker must have valid administrative credentials.		
CVE-2025-36059	ibm - Business Automation Workflow containers	IBM Business Automation Workflow containers 25.0.0 through 25.0.0 Interim Fix 002, 24.0.1 through 24.0.1 Interim Fix 005, and 24.0.0 through 24.0.0 Interim Fix 006. IBM Cloud Pak for Business Automation could allow a local user with access to the container to execute OS system calls.	2026-01-20	4.7
CVE-2026-21981	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.6 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:L).	2026-01-20	4.6
CVE-2026-21975	oracle - multiple products	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.29 and 21.3-21.20. Easily exploitable vulnerability allows high privileged attacker having Authenticated User privilege with network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java VM. CVSS 3.1 Base Score 4.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H).	2026-01-20	4.5
CVE-2026-22275	dell - ObjectScale	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0, contains an Inclusion of Sensitive Information in Source Code vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	2026-01-23	4.4
CVE-2026-22279	dell - powerscale_onefs	Dell PowerScale OneFS, versions prior 9.13.0.0, contains an insufficient logging vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information tampering.	2026-01-22	4.3
CVE-2025-46699	dell - data_protection_advisor	Dell Data Protection Advisor, versions prior to 19.12, contains an Improper Neutralization of Special Elements Used in a Template Engine vulnerability in the Server. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2026-01-23	4.3
CVE-2026-21922	oracle - planning_and_budgeting_cloud_service	Vulnerability in the Oracle Planning and Budgeting Cloud Service product of Oracle Hyperion (component: EPM Agent). The supported version that is affected is 25.04.07. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Planning and Budgeting Cloud Service executes to compromise Oracle Planning and Budgeting Cloud Service. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Planning and Budgeting Cloud Service accessible data. Note: Update EPM Agent. Please refer to <a href="https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/diepm/epm_agent_downloading_agent_110x80569d70.html">Downloading the EPM Agent for more information. CVSS 3.1 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N).	2026-01-20	4.2
CVE-2026-0988	red hat - multiple products	A flaw was found in glib. Missing validation of offset and count parameters in the g_buffered_input_stream_peek() function can lead to an integer overflow during length calculation. When specially crafted values are provided, this overflow results in an incorrect size being passed to memcpy(), triggering a buffer overflow. This can cause application crashes, leading to a Denial of Service (DoS).	2026-01-21	3.7
CVE-2025-36411	ibm - applinx	IBM ApplinX 11.1 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.	2026-01-20	3.5
CVE-2026-22281	dell - multiple products	Dell PowerScale OneFS, versions 9.5.0.0 through 9.5.1.5, versions 9.6.0.0 through 9.7.1.10, versions 9.8.0.0 through 9.10.1.3, versions starting from 9.11.0.0 and prior to 9.13.0.0, contains a Time-of-check Time-of-use (TOCTOU) race condition vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to denial of service.	2026-01-22	3.5
CVE-2025-36410	ibm - applinx	IBM ApplinX 11.1 could allow an authenticated user to perform unauthorized administrative actions on the server due to server-side enforcement of client-side security.	2026-01-20	3.1
CVE-2026-21947	oracle - multiple products	Vulnerability in Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u471-b50. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. 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 accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	2026-01-20	3.1
CVE-2026-1035	red hat - multiple products	A flaw was found in the Keycloak server during refresh token processing, specifically in the TokenManager class responsible for enforcing refresh token reuse policies. When strict refresh token rotation is enabled, the validation and update of refresh token usage are not performed atomically. This allows concurrent refresh requests to bypass single-use enforcement and issue multiple access tokens from the same refresh token. As a result, Keycloak's refresh token rotation hardening can be undermined.	2026-01-21	3.1

CVE-2026-21965	oracle - mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 9.0.0-9.5.0. 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2026-01-20	2.7
CVE-2025-14083	red hat - Red Hat Build of Keycloak	A flaw was found in the Keycloak Admin REST API. This vulnerability allows the exposure of backend schema and rules, potentially leading to targeted attacks or privilege escalation via improper access control.	2026-01-21	2.7
CVE-2026-21930	oracle - sun_zfs_storage_appliance_kit	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Filesystems). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 2.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2026-01-20	2.3
131				
132				
133				
134				
135				
136				
137				
138				
139				
140				
141				
142				
143				
144				
145				
146				
147				
148				
149				
150				
151				
152				
153				
154				
155				
156				
157				
158				
159				
160				
161				
162				
163				
164				
165				
166				
167				
168				
169				
170				
171				
172				
173				
174				
175				
176				
177				
178				
179				
180				
181				
182				
183				
184				
185				
186				
187				
188				
189				
190				
191				

192				
193				
194				
195				
196				
197				
198				
199				
200				
201				
202				
203				
204				
205				
206				
207				
208				
209				
210				
211				
212				
213				
214				
215				
216				
217				
218				
219				
220				
221				
222				
223				
224				
225				
226				
227				
228				
229				
230				
231				
232				
233				
234				
235				
236				
237				
238				
239				
240				
241				
242				
243				
244				
245				
246				
247				
248				
249				
250				
251				
252				
253				
254				
255				
256				
257				
258				
259				
260				
261				
262				
263				
264				
265				
266				
267				
268				

269				
270				
271				
272				
273				
274				
275				
276				
277				
278				
279				
280				
281				
282				
283				
284				
285				
286				
287				
288				
289				
290				
290				
291				
292				
293				
294				
295				
296				
297				
298				

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.