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 13th of July to 19th of July. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

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 ١٣ يوليو إلى ١٩ يوليو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية 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-2025-20337	cisco - multiple products	A vulnerability in a specific API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to execute arbitrary code on the underlying operating system as root. The attacker does not require any valid credentials to exploit this vulnerability. _ This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted API request. A successful exploit could allow the attacker to obtain root privileges on an affected device.	2025-07-16	10
CVE-2025-49746	microsoft - Azure Machine Learning	Improper authorization in Azure Machine Learning allows an authorized attacker to elevate privileges over a network.	2025-07-18	9.9
CVE-2025-49747	microsoft - Azure Machine Learning	Missing authorization in Azure Machine Learning allows an authorized attacker to elevate privileges over a network.	2025-07-18	9.9
CVE-2025-52688	alcatel-lucent - OmniAccess Stellar Products	Successful exploitation of the vulnerability could allow an attacker to inject commands with root privileges on the access point, potentially leading to the loss of confidentiality, integrity, availability, and full control of the access point.	2025-07-16	9.8
CVE-2025-52689	alcatel-lucent - OmniAccess Stellar Products	Successful exploitation of the vulnerability could allow an unauthenticated attacker to obtain a valid session ID with administrator privileges by spoofing the login request, potentially allowing the attacker to modify the behaviour of the access point.	2025-07-16	9.8
CVE-2025-7673	zyxel - VMG8825-T50K firmware	A buffer overflow vulnerability in the URL parser of the zhttpd web server in Zyxel VMG8825-T50K firmware versions prior to V5.50(ABOM.5)C0 could allow an unauthenticated attacker to cause denial-of-service (DoS) conditions and potentially execute arbitrary code by sending a specially crafted HTTP request.	2025-07-16	9.8
CVE-2025-25257	fortinet - multiple products	An improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability [CWE-89] in Fortinet FortiWeb version 7.6.0 through 7.6.3, 7.4.0 through 7.4.7, 7.2.0 through 7.2.10 and below 7.0.10 allows an unauthenticated attacker to execute unauthorized SQL code or commands via crafted HTTP or HTTPs requests.	2025-07-17	9.8
CVE-2025-41236	vmware - multiple products	VMware ESXi, Workstation, and Fusion contain an integer-overflow vulnerability in the VMXNET3 virtual network adapter. A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host. Non VMXNET3 virtual adapters are not affected by this issue.	2025-07-15	9.3
CVE-2025-41237	vmware - multiple products	VMware ESXi, Workstation, and Fusion contain an integer-underflow in VMCI (Virtual Machine Communication Interface) that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.	2025-07-15	9.3
CVE-2025-41238	vmware - multiple products	VMware ESXi, Workstation, and Fusion contain a heap-overflow vulnerability in the PVSCSI (Paravirtualized SCSI) controller that leads to an out of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox and exploitable only with configurations that are unsupported. On Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.	2025-07-15	9.3
CVE-2025-34125	d-link - DSP-W110A1	An unauthenticated command injection vulnerability exists in the cookie handling process of the lighttpd web server on D-Link DSP-W110A1 firmware version 1.05B01. This occurs when specially	2025-07-16	9.3

		crafted cookie values are processed, allowing remote attackers to execute arbitrary commands on the underlying Linux operating system. Successful exploitation enables full system compromise.		
CVE-2025-50067	oracle - multiple products	Vulnerability in Oracle Application Express (component: Strategic Planner Starter App). Supported versions that are affected are 24.2.4 and 24.2.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Application Express. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).	2025-07-15	9
CVE-2025-47158	microsoft - Azure DevOps	Authentication bypass by assumed-immutable data in Azure DevOps allows an unauthorized attacker to elevate privileges over a network.	2025-07-18	9
CVE-2025-53689	apache software foundation - Apache Jackrabbit	Blind XXE Vulnerabilities in jackrabbit-spi-commons and jackrabbit-core in Apache Jackrabbit < 2.23.2 due to usage of an unsecured document build to load privileges. Users are recommended to upgrade to versions 2.20.17 (Java 8), 2.22.1 (Java 11) or 2.23.2 (Java 11, beta versions), which fix this issue. Earlier versions (up to 2.20.16) are not supported anymore, thus users should update to the respective supported version.	2025-07-14	8.8
CVE-2025-6558	google - chrome	Insufficient validation of untrusted input in ANGLE and GPU in Google Chrome prior to 138.0.7204.157 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2025-07-15	8.8
CVE-2025-7656	google - chrome	Integer overflow in V8 in Google Chrome prior to 138.0.7204.157 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2025-07-15	8.8
CVE-2025-7657	google - chrome	Use after free in WebRTC in Google Chrome prior to 138.0.7204.157 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2025-07-15	8.8
CVE-2025-30751	oracle - multiple products	Vulnerability in the Oracle Database component of Oracle Database Server. Supported versions that are affected are 19.3-19.27 and 23.4-23.8. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Oracle Database. Successful attacks of this vulnerability can result in takeover of Oracle Database. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2025-07-15	8.8
CVE-2024-13972	sophos - Sophos Intercept X for Windows	A vulnerability related to registry permissions in the Intercept X for Windows updater prior to version 2024.3.2 can lead to a local user gaining SYSTEM level privileges during a product upgrade.	2025-07-17	8.8
CVE-2025-7433	sophos - Sophos Intercept X for Windows	A local privilege escalation vulnerability in Sophos Intercept X for Windows with Central Device Encryption 2025.1 and older allows arbitrary code execution.	2025-07-17	8.8
CVE-2025-53762	microsoft - Microsoft Purview	Permissive list of allowed inputs in Microsoft Purview allows an authorized attacker to elevate privileges over a network.	2025-07-18	8.7
CVE-2025-0886	lenovo - multiple products	An incorrect permissions vulnerability was reported in Elliptic Labs Virtual Lock Sensor that could allow a local, authenticated user to escalate privileges.	2025-07-17	8.5
CVE-2025-6231	lenovo - multiple products	An improper validation vulnerability was reported in Lenovo Vantage that under certain conditions could allow a local attacker to execute code with elevated permissions by modifying an application configuration file.	2025-07-17	8.5
CVE-2025-6232	lenovo - multiple products	An improper validation vulnerability was reported in Lenovo Vantage that under certain conditions could allow a local attacker to execute code with elevated permissions by modifying specific registry locations.	2025-07-17	8.5
CVE-2025-4657	lenovo - multiple products	A buffer overflow vulnerability was reported in the Lenovo Protection Driver, prior to version 5.1.1110.4231, used in Lenovo PC Manager, Lenovo Browser, and Lenovo App Store could allow a local attacker with elevated privileges to execute arbitrary code.	2025-07-17	8.4
CVE-2025-6249	lenovo - FileZ Client	An authentication bypass vulnerability was reported in FileZ client application that could allow a local attacker with elevated permissions access to application data.	2025-07-17	8.4
CVE-2025-53024	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. 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).	2025-07-15	8.2
CVE-2025-53027	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. 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).	2025-07-15	8.2
CVE-2025-53028	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. 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).	2025-07-15	8.2
CVE-2025-30744	oracle - mobile_field_service	Vulnerability in the Oracle Mobile Field Service product of Oracle E-Business Suite (component: Multiplatform Sync Errors). 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 Mobile Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Mobile Field Service accessible data as well as unauthorized access to critical data or complete access to all Oracle Mobile Field	2025-07-15	8.1

		Service accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).		
CVE-2025-50060	oracle - multiple products	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 7.6.0.0.0, 8.2.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle BI Publisher accessible data as well as unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2025-07-15	8.1
CVE-2025-50105	oracle - universal_work_queue	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Administration). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Universal Work Queue accessible data as well as unauthorized access to critical data or complete access to all Oracle Universal Work Queue accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2025-07-15	8.1
CVE-2025-52690	alcatel-lucent - OmniAccess Stellar Products	Successful exploitation of the vulnerability could allow an attacker to execute arbitrary commands as root, potentially leading to the loss of confidentiality, integrity, availability, and full control of the access point.	2025-07-16	8.1
CVE-2025-6023	grafana - Grafana	An open redirect vulnerability has been identified in Grafana OSS that can be exploited to achieve XSS attacks. The vulnerability was introduced in Grafana v11.5.0. The open redirect can be chained with path traversal vulnerabilities to achieve XSS. Fixed in versions 12.0.2+security-01, 11.6.3+security-01, 11.5.6+security-01, 11.4.6+security-01 and 11.3.8+security-01	2025-07-18	7.6
CVE-2025-30762	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2025-07-15	7.5
CVE-2025-36097	ibm - multiple products	IBM WebSphere Application Server 9.0 and WebSphere Application Server Liberty 17.0.0.3 through 25.0.0.7 are vulnerable to a denial of service, caused by a stack-based overflow. An attacker can send a specially crafted request that cause the server to consume excessive memory resources.	2025-07-16	7.5
CVE-2025-7472	sophos - Sophos Intercept X for Windows Installer	A local privilege escalation vulnerability in the Intercept X for Windows installer prior version 1.22 can lead to a local user gaining system level privileges, if the installer is run as SYSTEM.	2025-07-17	7.5
CVE-2025-6265	zyxel - NWA50AX PRO firmware	A path traversal vulnerability in the file_upload-cgi CGI program of Zyxel NWA50AX PRO firmware version 7.10(ACGE.2) and earlier could allow an authenticated attacker with administrator privileges to access specific directories and delete files, such as the configuration file, on the affected device.	2025-07-15	7.2
CVE-2025-41239	vmware - multiple products	VMware ESXi, Workstation, Fusion, and VMware Tools contains an information disclosure vulnerability due to the usage of an uninitialised memory in vSockets. A malicious actor with local administrative privileges on a virtual machine may be able to exploit this issue to leak memory from processes communicating with vSockets.	2025-07-15	7.1
CVE-2025-37104	hewlett packard enterprise (hpe) - HPE Telco Service Orchestrator	A security vulnerability has been identified in HPE Telco Service Orchestrator software. The vulnerability could allow authenticated clients to to perform a SQL Injection attack when sending a service request, and potentially exfiltrate the database's vendor name to unauthorized authenticated clients.	2025-07-16	7.1
CVE-2025-6248	lenovo - Browser	A cross-site scripting (XSS) vulnerability was reported in the Lenovo Browser that could allow an attacker to obtain sensitive information if a user visits a web page with specially crafted content.	2025-07-17	7.1
CVE-2025-50068	oracle - multiple products	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2025-07-15	6.7
CVE-2024-27779	fortinet - multiple products	An insufficient session expiration vulnerability [CWE-613] in FortiSandbox FortiSandbox version 4.4.4 and below, version 4.2.6 and below, 4.0 all versions, 3.2 all versions and FortiIsolator version 2.4 and below, 2.3 all versions, 2.2 all versions, 2.1 all versions, 2.0 all versions, 1.2 all versions may allow a remote attacker in possession of an admin session cookie to keep using that admin's session even after the admin user was deleted.	2025-07-18	6.7
CVE-2025-52080	netgear - xr300_firmware	In Netgear XR300 V1.0.3.38_10.3.30, a stack-based buffer overflow vulnerability exists in the HTTPD service through the usb_device.cgi endpoint. The vulnerability occurs when processing POST requests containing the share_name parameter.	2025-07-15	6.5
CVE-2025-52081	netgear - xr300_firmware	In Netgear XR300 V1.0.3.38_10.3.30, a stack-based buffer overflow vulnerability exists in the HTTPD service through the usb_device.cgi endpoint. The vulnerability occurs when processing POST requests containing the usb_folder parameter.	2025-07-15	6.5
CVE-2025-52082	netgear - xr300_firmware	In Netgear XR300 V1.0.3.38_10.3.30, a stack-based buffer overflow exists in the HTTPD service through the usb_device.cgi endpoint. The vulnerability occurs when processing POST requests containing the read_access parameter.	2025-07-15	6.5
CVE-2025-30753	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1	2025-07-15	6.5

		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).		
CVE-2025-50076	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.0-8.0.25. 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).	2025-07-15	6.5
CVE-2025-50078	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	6.5
CVE-2025-50082	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	6.5
CVE-2025-50083	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	6.5
CVE-2025-20283	cisco - multiple products	A vulnerability in a specific API of Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to execute arbitrary code on the underlying operating system as root._ _ This vulnerability is due to insufficient validation of user-supplied input. An attacker with valid credentials could exploit this vulnerability by submitting a crafted API request. A successful exploit could allow the attacker to execute commands as the root user. To exploit this vulnerability, the attacker must have valid high-privileged credentials.	2025-07-16	6.5
CVE-2025-20284	cisco - multiple products	A vulnerability in a specific API of Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to execute arbitrary code on the underlying operating system as root._ _ This vulnerability is due to insufficient validation of user-supplied input. An attacker with valid credentials could exploit this vulnerability by submitting a crafted API request. A successful exploit could allow the attacker to execute commands as the root user. To exploit this vulnerability, the attacker must have valid high-privileged credentials.	2025-07-16	6.5
CVE-2025-7784	red hat - multiple products	A flaw was found in the Keycloak identity and access management system when Fine-Grained Admin Permissions(FGAPv2) are enabled. An administrative user with the manage-users role can escalate their privileges to realm-admin due to improper privilege enforcement. This vulnerability allows unauthorized elevation of access rights, compromising the intended separation of administrative duties and posing a security risk to the realm.	2025-07-18	6.5
CVE-2025-47995	microsoft - Azure Machine Learning	Weak authentication in Azure Machine Learning allows an authorized attacker to elevate privileges over a network.	2025-07-18	6.5
CVE-2025-33097	ibm - QRadar SIEM	IBM QRadar SIEM 7.5 - 7.5.0 UP12 IF02 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-07-15	6.4
CVE-2025-50071	oracle - applications_framework	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Web Utilities). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. While the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N).	2025-07-15	6.4
CVE-2025-20274	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center could allow an authenticated, remote attacker to upload arbitrary files to an affected device._ _ This vulnerability is due to improper validation of files that are uploaded to the web-based management interface. An attacker could exploit this vulnerability by uploading arbitrary files to an affected device. A successful exploit could allow the attacker to store malicious files on the system and execute arbitrary commands on the operating system. The Security Impact Rating (SIR) of this advisory has been raised to High because an attacker could elevate privileges to root. To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of Report Designer.	2025-07-16	6.3
CVE-2025-30746	oracle - istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.2.3-12.2.14. 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).	2025-07-15	6.1

CVE-2025-30748	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). 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).	2025-07-15	6.1
CVE-2025-30756	oracle - rest_data_services	Vulnerability in Oracle REST Data Services (component: General). The supported version that is affected is 24.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle REST Data Services. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle REST Data 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 REST Data Services accessible data as well as unauthorized read access to a subset of Oracle REST Data Services 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).	2025-07-15	6.1
CVE-2025-30759	oracle - multiple products	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Platform Security). Supported versions that are affected are 7.6.0.0.0, 8.2.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 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).	2025-07-15	6.1
CVE-2025-50073	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.4.0, 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 WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2025-07-15	6.1
CVE-2025-50107	oracle - universal_work_queue	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Request handling). Supported versions that are affected are 12.2.5-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Universal Work Queue, 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 Universal Work Queue accessible data as well as unauthorized read access to a subset of Oracle Universal Work Queue 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).	2025-07-15	6.1
CVE-2025-22227	vmware - Reactor Netty	In some specific scenarios with chained redirects, Reactor Netty HTTP client leaks credentials. In order for this to happen, the HTTP client must have been explicitly configured to follow redirects.	2025-07-16	6.1
CVE-2025-53025	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. 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).	2025-07-15	6
CVE-2025-53026	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. 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).	2025-07-15	6
CVE-2025-53030	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. 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).	2025-07-15	6
CVE-2025-6491	php - multiple products	In PHP versions:8.1.* before 8.1.33, 8.2.* before 8.2.29, 8.3.* before 8.3.23, 8.4.* before 8.4.10 when parsing XML data in SOAP extensions, overly large (>2Gb) XML namespace prefix may lead to null pointer dereference. This may lead to crashes and affect the availability of the target server.	2025-07-13	5.9

CVE-2025-1735	php - multiple products	In PHP versions:8.1.* before 8.1.33, 8.2.* before 8.2.29, 8.3.* before 8.3.23, 8.4.* pgsql and pdo_pgsql escaping functions do not check if the underlying quoting functions returned errors. This could cause crashes if Postgres server rejects the string as invalid.	2025-07-13	5.9
CVE-2025-20288	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center could allow an unauthenticated, remote attacker to conduct a server-side request forgery (SSRF) attack through an affected device._ _ This vulnerability is due to improper input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected device.	2025-07-16	5.8
CVE-2025-48795	apache software foundation - Apache CXF	Apache CXF stores large stream based messages as temporary files on the local filesystem. A bug was introduced which means that the entire temporary file is read into memory and then logged. An attacker might be able to exploit this to cause a denial of service attack by causing an out of memory exception. In addition, it is possible to configure CXF to encrypt temporary files to prevent sensitive credentials from being cached unencrypted on the local filesystem, however this bug means that the cached files are written out to logs unencrypted. Users are recommended to upgrade to versions 3.5.11, 3.6.6, 4.0.7 or 4.1.1, which fixes this issue.	2025-07-15	5.6
CVE-2025-30483	dell - multiple products	Dell ECS versions prior to 3.8.1.5/ ObjectScale version 4.0.0.0 contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2025-07-15	5.5
CVE-2025-50085	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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 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).	2025-07-15	5.5
CVE-2025-30760	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 9.2.0.0-9.2.9.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2025-07-15	5.4
CVE-2025-50061	oracle - multiple products	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 20.12.0-20.12.21, 21.12.0-21.12.21, 22.12.0-22.12.19, 23.12.0-23.12.13 and 24.12.0-24.12.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio 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 Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management 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).	2025-07-15	5.4
CVE-2025-50090	oracle - e-business_suite	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Personalization). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 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).	2025-07-15	5.4
CVE-2025-50108	oracle - hyperion_financial_reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Workspace). The supported version that is affected is 11.2.20.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Financial Reporting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting 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).	2025-07-15	5.4
CVE-2025-46959	adobe - multiple products	Adobe Experience Manager versions 6.5.22 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. A low privileged attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a specially crafted web page.	2025-07-16	5.4
CVE-2025-47053	adobe - multiple products	Adobe Experience Manager versions 6.5.22 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. A low privileged attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser.	2025-07-16	5.4

		Exploitation of this issue requires user interaction in that a victim must visit a specially crafted web page.		
CVE-2025-1729	lenovo - TrackPoint Quick Menu	A DLL hijacking vulnerability was reported in TrackPoint Quick Menu software that, under certain conditions, could allow a local attacker to escalate privileges.	2025-07-17	5.4
CVE-2025-33014	ibm - multiple products	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.7 and 6.2.0.0 through 6.2.0.4 uses a web link with untrusted references to an external site. A remote attacker could exploit this vulnerability to expose sensitive information or perform unauthorized actions on the victims' web browser.	2025-07-18	5.4
CVE-2025-50070	oracle - database_server	Vulnerability in the JDBC component of Oracle Database Server. Supported versions that are affected are 23.4-23.8. Difficult to exploit vulnerability allows low privileged attacker having Authenticated OS User privilege with logon to the infrastructure where JDBC executes to compromise JDBC. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JDBC, 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 JDBC accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:N/A:N).	2025-07-15	5.3
CVE-2025-53031	oracle - multiple products	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.8, 8.0.8.5, 8.0.8.6, 8.1.1.4 and 8.1.2.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure 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).	2025-07-15	5.3
CVE-2025-7836	d-link - DIR-816L	A vulnerability has been found in D-Link DIR-816L up to 2.06B01 and classified as critical. Affected by this vulnerability is the function lxmldbc_system of the file /htdocs/cgibin of the component Environment Variable Handler. The manipulation leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-07-19	5.3
CVE-2025-50077	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50079	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50080	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50084	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50086	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50087	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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 creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).	2025-07-15	4.9
CVE-2025-50088	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. 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).	2025-07-15	4.9
CVE-2025-50089	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or	2025-07-15	4.9

		frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).		
CVE-2025-50091	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50092	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50093	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50094	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.42, 8.4.5 and 9.3.0. 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).	2025-07-15	4.9
CVE-2025-50095	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50097	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50099	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50101	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-50102	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	4.9
CVE-2025-53023	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.0-8.0.42. 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).	2025-07-15	4.9
CVE-2025-53032	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2025-07-15	4.9
CVE-2025-7545	gnu - Binutils	A vulnerability classified as problematic was found in GNU Binutils 2.45. Affected by this vulnerability is the function copy_section of the file binutils/objcopy.c. The manipulation leads to heap-based buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The patch is named 08c3cbe5926e4d355b5cb70bbec2b1eeb40c2944. It is recommended to apply a patch to fix this issue.	2025-07-13	4.8
CVE-2025-7546	gnu - Binutils	A vulnerability, which was classified as problematic, has been found in GNU Binutils 2.45. Affected by this issue is the function bfd_elf_set_group_contents of the file bfd/elf.c. The manipulation leads to out-of-bounds write. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The name of the patch is 41461010eb7c79fee7a9d5f6209accdaac66cc6b. It is recommended to apply a patch to fix this issue.	2025-07-13	4.8

CVE-2025-50064	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 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).	2025-07-15	4.8
CVE-2025-6230	lenovo - multiple products	A SQL injection vulnerability was reported in Lenovo Vantage that could allow a local attacker to modify the local SQLite database and execute code with elevated permissions.	2025-07-17	4.8
CVE-2025-50096	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2025-07-15	4.4
CVE-2025-50103	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 9.0.0-9.3.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2025-07-15	4.4
CVE-2025-30747	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). 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. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N).	2025-07-15	4.3
CVE-2025-20272	cisco - multiple products	A vulnerability in a subset of REST APIs of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, low-privileged, remote attacker to conduct a blind SQL injection attack._ _ This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to an affected API. A successful exploit could allow the attacker to view data in some database tables on an affected device.	2025-07-16	4.3
CVE-2025-3415	grafana - Grafana	Grafana is an open-source platform for monitoring and observability. The Grafana Alerting DingDing integration was not properly protected and could be exposed to users with Viewer permission. Fixed in versions 10.4.19+security-01, 11.2.10+security-01, 11.3.7+security-01, 11.4.5+security-01, 11.5.5+security-01, 11.6.2+security-01 and 12.0.1+security-01	2025-07-17	4.3
CVE-2024-32124	fortinet - multiple products	An improper access control vulnerability [CWE-284] in FortiIsolator version 2.4.4, version 2.4.3, 2.3 all versions logging component may allow a remote authenticated read-only attacker to alter logs via a crafted HTTP request.	2025-07-18	4.3
CVE-2025-24477	fortinet - multiple products	A heap-based buffer overflow in Fortinet FortiOS versions 7.6.0 through 7.6.2, 7.4.0 through 7.4.7, 7.2.4 through 7.2.11 allows an attacker to escalate its privileges via a specially crafted CLI command	2025-07-15	4.2
CVE-2025-6197	grafana - Grafana	An open redirect vulnerability has been identified in Grafana OSS organization switching functionality. Prerequisites for exploitation: - Multiple organizations must exist in the Grafana instance - Victim must be on a different organization than the one specified in the URL	2025-07-18	4.2
CVE-2025-20285	cisco - multiple products	A vulnerability in the IP Access Restriction feature of Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to bypass configured IP access restrictions and log in to the device from a disallowed IP address._ _ This vulnerability is due to improper enforcement of access controls that are configured using the IP Access Restriction feature. An attacker could exploit this vulnerability by logging in to the API from an unauthorized source IP address. A successful exploit could allow the attacker to gain access to the targeted device from an IP address that should have been restricted. To exploit this vulnerability, the attacker must have valid administrative credentials.	2025-07-16	4.1
CVE-2025-50072	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle WebLogic Server executes to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 4.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	2025-07-15	4
CVE-2025-1220	php - multiple products	In PHP versions:8.1.* before 8.1.33, 8.2.* before 8.2.29, 8.3.* before 8.3.23, 8.4.* before 8.4.10 some functions like fsockopen() lack validation that the hostname supplied does not contain null characters. This may lead to other functions like parse_url() treat the hostname in different way, thus opening way to security problems if the user code implements access checks before access using such functions.	2025-07-13	3.7

CVE-2025-50081	oracle - multiple products	Vulnerability in the MySQL Client product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. 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 MySQL Client accessible data as well as unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N).	2025-07-15	3.1
CVE-2025-50066	oracle - multiple products	Vulnerability in the Oracle Database Materialized View component of Oracle Database Server. Supported versions that are affected are 19.3-19.27, 21.3-21.18 and 23.4-23.8. Easily exploitable vulnerability allows high privileged attacker having Execute on DBMS_REDEFINITION privilege with network access via Oracle Net to compromise Oracle Database Materialized View. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database Materialized View 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).	2025-07-15	2.7
CVE-2025-50098	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	2.7
CVE-2025-50104	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. 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).	2025-07-15	2.7
CVE-2025-52687	alcatel-lucent - OmniAccess Stellar	Successful exploitation of the vulnerability could allow an attacker with administrator credentials for the access point to inject malicious JavaScript into the payload of web traffics, potentially leading to session hijacking and denial-of-service (DoS).	2025-07-16	2.4
CVE-2025-53029	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox 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).	2025-07-15	2.3
CVE-2025-50100	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2025-07-15	2.2

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.